THE SECURITY RISKS ASSOCIATED WITH USING A MOBILE APPLICATON TO COLLECT WORK ORDER DATA

THESIS

Michael W. Peterson, Captain, USAF

AFIT-ENV-MS-17-M-213

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT-ENV-MS-17-M-213

THE SECURITY RISKS ASSOCIATED WITH USING A MOBILE APPLICATON TO COLLECT WORK ORDER DATA

THESIS

Presented to the Faculty

Department of Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Engineering Management

Michael W. Peterson, BS

Captain, USAF

March 2017

AFIT-ENY-MS-15-M-213

THE SECURITY RISKS ASSOCIATED WITH USING A MOBILE APPLICATON TO COLLECT WORK ORDER DATA

Michael W. Peterson, BS

Captain, USAF

Committee Membership:

Dr. B. T. Langhals, PhD
Chair

Dr. J. E. Elshaw, PhD
Member

Dr. D. V. Prigge, PhD
Member

AFIT-ENY-MS-15-M-213

Abstract

The use of smart phone technology may be able to improve the Air Force's ability to sustain infrastructure, reduce costs and redundancy, and provide a more accurate sustainment budget forecast by using a mobile application to collect infrastructure deficiencies. However, before any such benefits can be realized, Air Force leaders need to know the security risks associated with the implementation of mobile technology.

According to Daft and Lengel (1986), "information richness is defined as the ability of information to change understanding within a time interval" (p. 560). The "richer" the communication medium, the more effective it is at changing understanding. In other words, the more learning that can be pumped through a medium, the richer the medium (Lengel & Draft, 1988). Based on media richness theory, a mobile application may be considered a "richer" form of communication. With additional richness and consequently more learning, are unintended operational security (OPSEC) cues transmitted via a mobile application as compared to traditional work order submission methods?

This uses OPSEC principles to evaluate security concerns associated with using a mobile application to collect work order data. An experiment was conducted to compare a mobile application to the traditional collection process. The results of that experiment provide significant evidence that the use of a mobile application increases the risk of capturing critical information. Therefore, in order to deploy such an application there needs to be a risk mitigation strategy and a training plan in place.

Acknowledgments

I would like to express my sincere appreciation to my thesis advisor, Dr. Brent Langhals, for his leadership and encouragement throughout the course of this thesis effort. His guidance, insight, and expertise were certainly appreciated. I would, also, like to thank the members of my thesis committee, Dr. John Elshaw and Dr. Diedrich Prigge, for their enthusiasm, commitment and invaluable feedback. This effort would not have been possible without the help of my entire research committee. Thank you all for your support and guidance throughout this endeavor.

Additionally, I would like to thank my friend and key member of my research team, Captain Victor Guinn. He not only provided professional and quality support to this research, but he made the experience enjoyable. I am forever grateful for his support and friendship. Finally, I am humbled and honored for the support and sacrifice of my wife, Marie, and son, Caleb. Their understanding, love, and support motivated me to accomplish more than I ever thought possible. Thank you.

Captain Michael W. Peterson

Table of Contents

Page

List of Figures

List of Tables

THE SECURITY RISKS ASSOCIATED WITH USING A MOBILE APPLICATON TO COLLECT WORK ORDER DATA

I. Introduction

Background

The outcome of any armed conflict is impacted by each side's ability to protect critical information. The side that possesses the most knowledge about their adversary's capability and intent will usually have a winning advantage. When a military or civilian organization fails to secure critical information, they are unintentionally giving away that advantage. During the Sixth Century BC, the famous Chinese General Sun Tzu wrote, in *The Art of War*, "what enables the wise and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge" (Giles, 1910, p. 59). It behooves us to ensure the enemy is blind to even the smallest details related to military operations through the protection of critical information.

In a military environment, information is typically considered classified or unclassified. There are processes in place to protect classified information. However, critical unclassified information can be difficult to identify and protect. Critical information is defined in Joint Publication 2-0 (2013) as, "Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment" (P. GL-6). Therefore, critical information is any information that an adversary can use to inflict harm or negatively impact the outcome of a mission.

This research evaluated the Air Force Civil Engineer (CE) work request collection process (WRCP) and looked for critical information that could exist within the process. Furthermore, the purpose was to investigate whether or not the use of a mobile application, as part of the collection process, could increases the risk of exposing critical information to an adversary. The Air Force's operational security process was used to identify critical information that could be compromised during the collection of work order data.

Operational Security (OPSEC)

Operational security (OPSEC) is defined by the Department of Defense (DoD) in Directive 5205.02 (2006) as, "A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities…" (p. 8). The process is used to protect critical unclassified information that can be used by an adversary to compromise military operations. As part of the process, the assessor(s) assumes an adversarial perspective to identify vulnerable information based on a military unit's specific mission and the capabilities of a potential adversary (Hatch, 1993). Therefore, the process is useful for identifying information that organizations want to protect.

Even though the term *operational security* was not formally defined until the Vietnam War Era, the concept has impacted every armed conflict throughout history—mainly because most military operations depend on the element of surprise, and even the smallest leak of information can expose intended actions or capabilities to the enemy (Hatch, 1993). The following is a summary of the declassified article titled "PURPLE DRAGON: The Origin and Development of the United States OPSEC Program" written by David A. Hatch (1993), former director of the Center for Cryptologic History, National Security Agency.

Most Americans are familiar with the story of Paul Revere and his famous ride, which alerted the Colonial militia that the British were attacking. His ride forewarned them about the imminent attack by the British prior to the battle of Lexington and Concord. That battle was the first armed military engagement of the American Revolutionary War. Surely the British leaders did not intend to alert the militia. However, simple changes in troop activity gave warning about the possibility of an attack (Hatch, 1993).

In Boston, 1775, British intelligence became aware of military supplies and weapons being stored in Concord. As they prepared for a march on Concord, they dismissed sentries from their normal post and repositioned transport boats from the harbor to the Boston shoreline. Furthermore, residents in Boston observed the soldiers participating in training events and military maneuvers. Having observed these changes in daily operations, Colonial leaders in Boston sent Paul Revere to give warning to Samuel Adams and John Hancock, who were stationed in Lexington (Hatch, 1993).

The Colonials were unaware of British intentions, but their change in normal operations indicated that an attack was probable. There were only a couple valuable military targets: the leadership stationed at Lexington or the military supplies stored at Concord. Hence, they established a warning system. If the British were to mobilize, Paul Revere and William Dawn would signal the event was taking place. On the night of 18 April 1775, that is just what they did (Hatch, 1993).

The British war ship, Somerset, was moved from the Boston harbor to the end of the Charles River, guards were deployed to control traffic on the main roads to Lexington, and soldiers secretly started to form-up. These signs lead the Colonials in Boston to assume imminent attack by the British; Revere and Dawn were dispatched to sound the alarm (Hatch, 1993).

The British did attack and they were seeking to destroy the military supplies. However, the Colonists' foreknowledge of the British attack allowed ample time for battle preparation. Military supplies were hidden, key personnel were moved, and the militia was readied. The British had no surprise attack and the Colonial militia defended the attack at Concord and defeated them at Lexington. The British retreated and they were subject to constant attack all the way back to Boston. Hence, the Colonials won the first battle of the American Revolution, because the British failed to protect critical information that provided foreknowledge of their intended operations. Their element of surprise and the battle were lost (Hatch, 1993).

Better Operational Security practices would have favored the British in the battle of Lexington and Concord. However, OPSEC did not exist as a formal process, until it was proven effective during the Vietnam War. During the war, airstrikes against the Viet Cong (VC) were becoming ineffective, and commanders on-the-ground wanted to know why. The prevailing hypothesis was that U.S. soldiers were inadvertently giving away information that allowed the VC to predict and avoid B-52 bomber targets (Hatch, 1993).

In 1966, Operation PURPLE DRAGON was born. Sanctioned by the U.S. Joint Chiefs of Staff, the purpose was to investigate mission planning from beginning to end and identify any information that could be useful to the enemy. The members of the operation put themselves in the position of the enemy to determine what vulnerabilities could be exploited. Most of the details about Operation PURPLE DRAGON are still classified. However, the operation successfully increased the effectiveness of military operation in Vietnam. Thus, a proven OPSEC process was born (Hatch, 1993).

In light of that success, the Joint Staff derived an Operational Security program using the model developed during PURPLE DRAGON. Later, President Ronald Reagan made OPSEC mandatory for any government agency with a national security mission (Hatch, 1993). Today OPSEC is a codified program published in DoD directive 5205.02 (2006).

Operational Security has been a valuable lessoned learned from history. This research used the OPSEC process to identify potential risks associated with gathering information about infrastructure deficiencies. Specifically, OPSEC literature was used to identify examples of critical information that could be inadvertently collected during the WRCP. The examples were used to design an experiment that tested whether or not a mobile application would increase the risk of collecting critical information.

Work Request Collection Process

Specific methods of managing the work request collection process vary between Air Force (AF) installations. However, the general concept is the same, because the CE mission stays the same. Civil Engineers are responsible for building and maintaining infrastructure on AF installations (Davis, 2013). Within a CE squadron, the Operations Engineering section manages the collection of work requests. A work request can be submitted for anything from fixing a leaking faucet to resurfacing an airfield or constructing a new facility. Customers submit work requests to personnel working in the Customer Service element of the Operations Engineering section (Davis, 2013).

In the Air Force, the *customer* is everyone on base who uses or occupies a particular facility or piece of infrastructure. For example, when a waterline breaks in a building, the occupant is the customer and they have a Facility Manager, who acts as a liaison between CE and the organization they represent. Facility Managers are trained to report infrastructure deficiencies and maintenance requirements to CE customer service. Each installation establishes specific methods for submitting work requests that best suits the operational environment and capability (Davis, 2013)

Traditionally, work requests are made via telephone, Internet, e-mail, or in-person. The information regarding the deficiency is communicated to the Customer Service element, and they establish a work order number and enter the request into a work order management system. The request should include a detailed description of the deficiency and may be accompanied by pictures and drawings that help describe the work required (Hasberry, 1991).

The traditional process of collecting infrastructure deficiencies (mainly via telephone and email) is struggling due to increased customer demand, amplified complexity of infrastructure issues, fewer personnel, and today’s high pace operations tempo. As a potential solution, mobile applications offer an additional method to collect work requests and report infrastructure deficiencies to CE customer service. However, are there additional security risks associated with using a mobile application to collect work order data? That is the question that motivates this research.

Mobile Applications

Some cities have successfully incorporated mobile applications into their public works departments in an effort to simplify and streamline the work request management process. Off-the-shelf commercial applications exist that allow citizens to report infrastructure deficiencies with the simple click of a button. All they need to do is download the application on their smart phone and start reporting infrastructure problems. For example, SeeClickFix is an application that allows residents to submit work requests and track repair status within their community (Collins, 2011).

A user simply submits a picture of the problem via the application and the location is automatically logged via the Global Positioning System (GPS) (Collins, 2011). It is becoming apparent that mobile applications will likely be used to collect work order data, thus the purpose of this research is to investigate the security risks associated with using a mobile application to collect work order data. There are many details on how mobile applications can be used to simplify the WRCP, and they will be thoroughly discussed in Chapter 2.

Research Purpose

Due to the AF's national security mission, introducing such an application would be complicated. The first thing a rightfully concerned Commander is going to ask; what are the security risks associated with utilizing the application? To begin to answer that question, we have to identify the vulnerabilities that exist within the information communicated through the existing and proposed processes.

In order to identify and evaluate OPSEC risks associated with the collection of infrastructure deficiency data, with particular regards to mobile applications vs traditional methods, an experiment was devised to collect and analyze the empirical data needed to answer the following question: *Does using a mobile application to collect work requests increase the risk of capturing critical information*? Answering the research question will help Air Force leaders make an informed decision when considering the use of a mobile application.

This research is unique because no other academic study has evaluated the WRCP using OPSEC principles. Furthermore, as information systems are becoming the "norm" for storing and transmitting information, there is an increasing need for a relevant risk assessment methodology. Today's leaders have to make decisions between increasing cybersecurity vulnerabilities and using information technology to increase mission effectiveness. This research developed a way to incorporate OPSEC principles into a specific risk assessment methodology.

Scope

The intent of this research was not to evaluate the effectiveness of a mobile application but rather focus on the risks associated with using one to collect work order data. Furthermore, it is not a study on Network Security, Communication Security, or Information Security. Using an OPSEC methodology, this study analyzed information specific to the WRCP and identified associated risks based on the existence of critical information and the probability of its collection.

Assumptions

The primary assumption is that using a mobile application will improve the WRCP and therefore will likely be used in the future and therefore must be evaluated from a security perspective. Also, it is assumed that the “adversary” has all the capabilities and required resources needed to exploit any potential security vulnerabilities that exist within the WRCP. For example, it is assumed that an adversary, if motivated, has the capability of accessing secured data (hacking) or intercepting phone conversations. Finally, it is assumed that the application will be used to communicate common minor repair issues that are typically called into CE Customer Service.

Approach and Methodology

A mixture of qualitative and quantitated methods was used to answer the research question. The question is: *Does using a mobile application to collect work requests increase the risk of capturing critical information*? First, OPSEC literature (qualitative) was used to identify potential critical information that may be present and collected along with the work order data. Second, an experiment was conducted using human subjects to submit work requests using the traditional (telephone) and mobile application methods. The response was the amount of pre-identified critical information that was actually captured by each method. Finally, a statistical analysis was conducted to determine if the application captured more critical information that the traditional method.

Application of Research

Air Force leaders can use the results of this research to support a decision on whether or not to use a mobile application to collect work order data. The results can also influence training on the use of a mobile application if approved for use. Additionally, the protection of critical information not only applies to military operations, it is also relevant in the private sector. In fact, civilian organizations are using OPSEC principles to protect proprietary information—especially within research and development industries (Pattakos, 2009). Therefore, this method of using OPSEC principles to identify risks and critical information is not only applicable to the military, but also the corporate world.

Summary

This chapter has provided a background on how the OPSEC process was developed and how it applies to this research. Furthermore, it briefly introduced the CE work request collection process (WRCP) and discussed how mobile applications can be incorporated into the process. Finally, this chapter described the purpose and objective of this research. Subsequent chapters will thoroughly describe the OPSEC process and its application in the military and corporate environment, explain more details about the WRCP, describe the functionality of the commercially used SeeClickFix application, introduce the media richness theory, and discuss the methodology used to design the experiment. Finally, Chapter 5 will explain the results of the experiment and make recommendations to leaders whom maybe considering using a mobile application to collect work order data.

II. Literature Review

Introduction

The purpose of this research is to assess the OPSEC-related security risks associated with using a mobile application as part of the work request collection process (WRCP). Air Force leaders have been working to improve mission effectiveness by transforming business practices and using new technologies (Eulberg, 2007). However, there is always hesitation to change, especially when dealing with new information systems and the associated cybersecurity challenges.

The current WRCP does not intentionally collect or transmit classified information. Infrastructure deficiencies such as a broken water line, leaking roof, or a power outage is not considered classified. Therefore, why not allow customers to report deficiencies via a mobile application? One reason, while work order data may not be classified it can still contain critical information that could be useful to an adversary.

Perhaps a customer is reporting a broken cooling system that supports communication equipment in a mission-critical facility. Imagine that the facility is an Air and Space Operations Center that supports command and control operations in an active war zone. Information about the location of the building, the type of mission that takes place in the building, and facility vulnerabilities aggregated together can lead to a significant security concern. Especially when there is a single point of failure that could degrade or hinder mission effectiveness. Therefore, anytime information is being transferred, OPSEC should be a constant consideration.

This research compares the use of a mobile application to the traditional work order process to determine if the application poses a greater risk of capturing critical information. The following review of literature will address how to identify security risks using the OPSEC process, describe the current method CE uses to collect infrastructure deficiencies, examine communication theory, and explain the functionality of a specific mobile application (SeeClickFix).

Relevant Research

The Operational Security Process (OPSEC)

For this research, the most relevant method of analyzing the security risks associated with unclassified information is the OPSEC process. The OPSEC methodology was created by the Department of Defense (DoD) to protect operation secrecy (Hatch, 1993). The process has been codified in several government publications, including: the "National Security Decision Directive 289" (1988), "Chairman of the Joint Chiefs of Staff Instruction 3213.01C" (2008), *Joint Publication 3-13.3* (2006), "Department of Defense Directive 5205.02" (2006), *Department of Defense Manual 5205.02* (2008), and *Air Force Instruction 10-701* (2011). The following section will explain the OPSEC process.

The OPSEC process is an analytical and proven method of identifying critical information in order to prevent adversaries from deriving information about "U.S. intentions, capabilities, operations, and activities" ("DoD Directive 5205.02," 2006). The overall goal of the process is to ensure mission effectiveness by achieving information supremacy and denying the enemy exploitable information ("AFI 10-701," 2011). Furthermore, the process is comprised of the five steps illustrated in Figure 1.

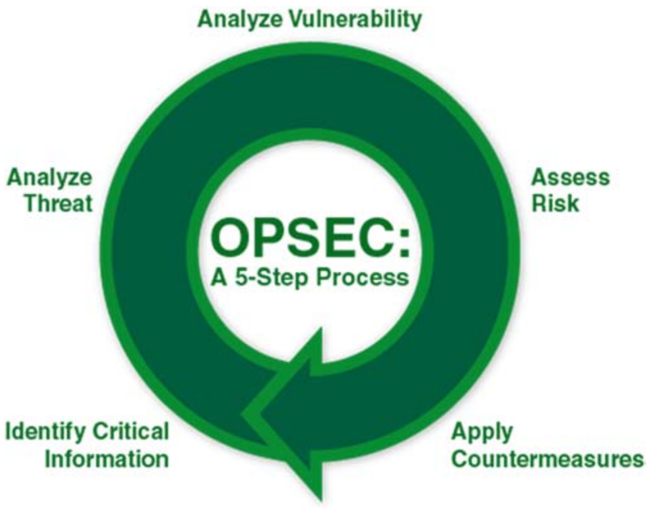


Figure 1. The OPSEC Process (U.S. Department of Agriculture, 2016)

Identifying critical information is the first step of the OPSEC process. In order to protect information from an adversary, you have to know what information is valuable to them ("Joint Publication [JP] 3-13.3," 2006). Critical information is defined in Joint Publication 3-13.3, *Operations Security*, as, "Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishment" (Ch. 2, p. 2). The first step is vital to the overall process, and it can be tailored to organizations depending on their specific mission ("DoD Manual [DoDM] 5205.02," 2008).

Critical information is unique to an organization and, depending on their mission, it may be hard to identify ("DoDM 5205.02," 2008). For example, it may be easier to identify information associated with a B-52 bomber strike (e.g. time and target) as critical versus logistical support information (e.g. capabilities and limitations). Both activities contain information that can be useful to an enemy. It may be easier to identify time and target as critical information. However, logistical capabilities and limitations can enable an adversary to predict the location and estimated timeframe of a planned attack (“JP 3-13.3,” 2006).

Critical information can be used to derive classified information just like “indicators” can identify sources of critical information (“JP 3-13.3,” 2006). The term *OPSEC indicator* is defined in Joint Publication 3-13.3 as, “Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information” (Ch. 2, p. 1). Several examples of critical information and indicators are listed in appendix A and B of Joint Publication 3-13.3. For this research, those examples and others were used to develop a list of indicators and critical information that are relevant to CE’s WRCP. Some of those relevant items were used to identify critical information within the experimental scenarios.

The second step of the OPSEC process is to *analyze the threat* (“JP 3-13.3,” 2006). During this part of the process, it is important to identify potential adversaries and gather as much information about them as possible. Critical information may be available, but different adversaries have varying degrees of motivation and competency. Therefore, the level of overall risk to your organization is relative to whom you identify as the adversary. The questions in Table 1 should be answered when conducting a threat analysis (“DoDM 5205.02,” 2008, p. 12).

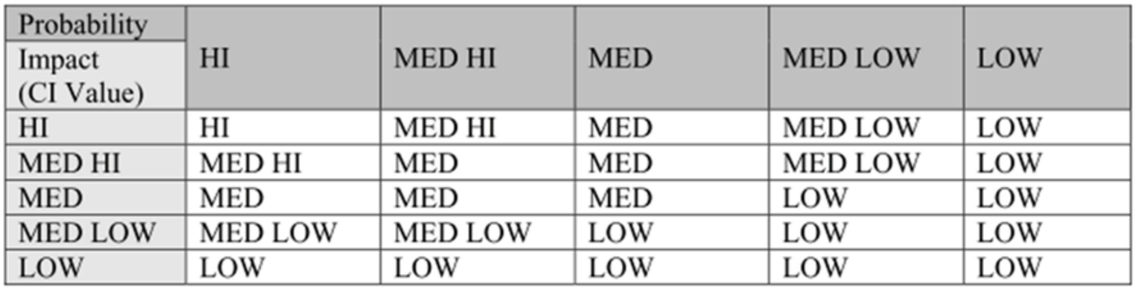
Table 1. Threat Analysis Questions (DoDM 5205.02, 2008, Appendix 1)

Number	Question
1	Who is the adversary?
2	What is the adversary's intent and capability?
3	What are the adversary's goals?
4	What tactics does the adversary use?
5	What does the adversary already know about the unit's mission?
6	What critical information has already been exposed and is known by the adversary?

The third step of the process is conducting an *analysis of vulnerabilities* ("JP 3-13.3," 2006). In this step, an individual uses the critical information and indicators identified in Step 1, and rates them based on how easy they are to exploit. For example, if the information is available on a public website, it would have a high vulnerability rating. Whereas, information stored on private servers would have a lower rating, because an adversary would have to either "hack" the network (assuming security protocols are in place) or solicit insider help to obtain the information. The more difficult the information is to obtain, the lower the vulnerability rating ("DoDM 5205.02," 2008).

Step 4 is the *assessment of risk* ("JP 3-13.3," 2006). Measurements from the previous three steps: *identify critical information* (including indicators), *conduct a threat analysis*, and *conduct a vulnerability assessment* are recorded and compared to determine the overall risk. The risk is measured based on the accessibility of information and how much it would affect the organizational mission. Table 2 is an example of a risk rating (low-high) derived from the probability of an adversary obtaining critical information and the potential mission impact resulting from an adversary exploiting critical information. The probability column is the result of using a similar assessment method that is based on the threat (adversary capability) and vulnerability (e.g. accessibility of information) (“DoDM 5205.02,” 2008).

Table 2. Risk Assessment (DoDM 5205.02, 2008)



Probability Impact (CI Value)	HI	MED HI	MED	MED LOW	LOW
HI	HI	MED HI	MED	MED LOW	LOW
MED HI	MED HI	MED	MED	MED LOW	LOW
MED	MED	MED	MED	LOW	LOW
MED LOW	MED LOW	MED LOW	LOW	LOW	LOW
LOW	LOW	LOW	LOW	LOW	LOW

The fifth and final step of the process is the *application of appropriate counter measures* (“JP 3-13.3,” 2006). Organization leaders must decide on implementing methods of protecting critical information based on the risk assessment rating and countermeasure costs. If the countermeasure is implemented, its effectiveness will be measured by conducting an operational security assessment. The OPSEC security assessment is defined in JP 3-13.3 as, “an intensive application of the OPSEC process to an existing operation or activity by a multidisciplinary team of experts” (Ch. 2, p. 6).

The first step of the OPSEC process is the most relevant to this research. It defines a process of identifying critical information and indicators of critical information. Several examples from the literature were used to identify critical information that has could exist within the WRCP. Additionally, the second step, analyzing the threat, shows that critical information will vary among different organizations depending on their specific mission and adversarial threat. Steps 3-5 are not extremely relevant to this research but could support follow-on research that investigates ways to protect critical information that exists within the WRCP. This research only addresses whether or not a mobile application is at risk for collecting more critical information that the traditional process.

Using OPSEC to Protect Corporate Assets

Government entities are not the only organizations that require secrecy to ensure successful operations. In a 2002 annual report to Congress, it was "estimated that US Fortune 1000 corporations may have lost more than $45 billion in 1999 from theft of their proprietary information" ("Office of the National Counterintelligence Executive," 2003, p. 1). Clearly, the OPSEC process can also be utilized by organizations outside the U.S. government.

In an article published in the *Journal of Corporate Treasury Management*, written by Burke L. Files (2009), an International Financial Investigator, he stated, "As a threat-based management process, operational security (OPSEC) is the most effective tool a company can use to protect its IPCI [or intellectual property and critical information]" (p. 298). In the article, he discussed the need to protect IPCI and how OPSEC can be used to prevent the loss of critical information (Files, 2009).

Files (2009) applied the OPSEC methodology to formulate a list of critical information that, if left unprotected, could be used by a competitor to steal IPCI. In comparison to a military operation, intellectual property (a form of proprietary information) is equivalent to classified military information. Therefore, identifying and protecting critical information in a corporate environment protects the company from threats (e.g. competitors) that would seek to steal the valuable IPCI. For example, a list of company employees and their information (phone number, address, e-mail, etc.) can be considered critical information. A competitor may be able to use such a list to coerce employees into revealing intellectual property or proprietary information (Files, 2009)

There is another source that translates the five-step OPSEC process into a risk management process for businesses. While working as the Director of Programs Integration for Beta Analytics International, retired Army Colonel, Arion N. Pattakos (1999), wrote an article titled, “The Operations Security Connection.” It was published in the *Program Manager Journal*. In the article, he described the OPSEC process and explained how corporate leaders and decision makers can use the process “to protect valued assets and information” (p. 38).

In addition, translating the OPSEC process, Pattakos (2009) explained “that some OPSEC practitioners look at the process through different lenses” (p. 37). The first lens is to look at the process as cyclical, as shown in Figure 1. The second perspective views the process as an overlapping Venn diagram (see Figure 2). When there is an overlap between critical assets, vulnerabilities, and threats, there is a need to protect the asset (Pattakos, 2009, p. 37).

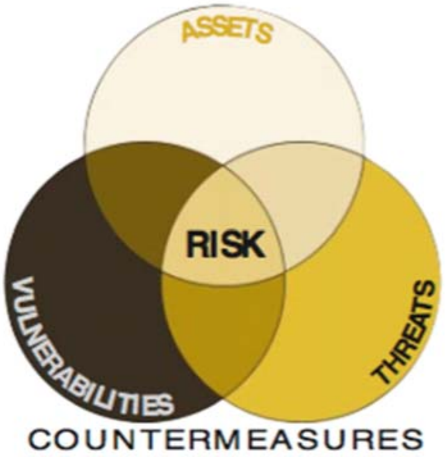


Figure 2. The OPSEC Process (Pattakos, 2009)

The OPSEC process is a five-step methodical procedure developed by the U.S. government to assess risks associated with military operations. It can also be used as a corporate risk management process. The process is a focal point of this research, because the work request collection process (WRCP) is a military process with national security interests. Similar to what Files (2009) did for civilian organizations, the OPSEC process and examples from the Appendix A and B of JP 3-13.3 (2006) were used to pre-identify critical information and indicators that existed within the experimental scenarios. These scenarios will be further discussed in Chapter 3.

Civil Engineering and the Work Request Collection Process (WRCP)

The WRCP is hereby defined as the method that the Air Force CE support function uses to collect information (from customers) about infrastructure deficiencies. A civil engineer squadron is responsible for building and sustaining base infrastructure and the Operations Management career field (customer service) is responsible for managing CE work requirements. With respect to the Air Force support functions, the customer is the entire population of an installation, and there are several ways that a customer can submit work requests to CE customer service (Davis, 2013).

Depending on the type of work being requested, a work request can be submitted via telephone, electronic or hard copy work request forms, e-mail, or in-person. In some cases a picture of the issue being reported is supplied or requested, however that is not normally the case. Regardless of the request method, the request should include a "detailed description of work, where to perform the work, and a point of contact (POC)" (Hasberry, 1991). Furthermore, if the justification for work is not evident, or there are factors that make the job "more important," a justification should be provided in order for

CE to prioritize the work. Critical information or indicators of critical information can exist within the WRCP.

For example, visualize a customer calling CE and requesting to have a door repaired on a legacy hardened-aircraft shelter that is no longer used to store aircraft. Assume the detailed description is that the door on the shelter is “jammed,” and the door cannot be closed. The customer provides a facility number and tells customer service that the shelter is located on the south side of the base. The request does not seem like an emergency. However, the customer insists that the door needs repaired, because the shelter is being used as a staging area for a special operations quick reaction force. Now that the customer provided sufficient justification, the work may be classified as urgent.

The fact that a door on an inactive, hardened aircraft shelter needs repaired is not critical information. However, the detail about Special Forces using the facility as a staging area provides evidence of a possible alert posture. Furthermore, an adversary may be interested in the type of equipment and supplies that are being stored. Staging locations, assigned forces, alert posture, and equipment capabilities are all examples of critical information (“JP 3-13.3,” 2006). The work request example above would be an indicator of critical information.

In the previous example, either method of collection (telephone or mobile application) may capture critical information. However, if a picture is taken via a mobile application, the picture may or may not reveal more information than the traditional call-in method. The purpose of this research is to determine if the mobile application increases OPSEC risk by collecting more critical information than the traditional method.

Mobile Applications

The number of people using electronic technologies and the capabilities of those technologies have been experiencing exponential growth. Banking, transportation, communication, entertainment, and much more have dramatically changed since the creation of computers and the Internet. Likewise, the use of mobile devices such as smart phones and tablets, along with high-speed wireless data transfer, is changing the way people live and how organizations conduct business. Furthermore, mobile information technology (IT) will continue to play a significant role in efforts to improve and innovate business processes (Sorensen et al., 2008).

Mobile computing technologies are being used as a tool to innovate the way private industry and government organizations conduct business. However, as it is with all technology, the added conveniences of mobile IT are accompanied by some additional security concerns. In an article titled “From Mobile Phones to Responsible Devices,” Traynor et al. (2011) stated, “mobile phone operating systems currently lack the mechanisms to adequately protect these increasingly capable devices” (p. 725). Furthermore, when it comes to mobile IT, “an adversary may be able to not only cause numerous violations of a user’s data confidentiality and device integrity, but also cause significant problems for the cellular networks themselves” (Traynor et al., 2011, p. 725). Therefore, even with state-of-the-art security, mobile computing comes with increased security risks—both to individual operators and corporate customers.

The scope of this research does not include computer security risks inherent to mobile IT and mobile applications but rather the OPSEC risks related to the data that are being collected. An experimental method was used to determine if the use of a mobile application increases the probability of collecting critical information when integrated into the WRCP. The experiment used two methods of collecting work requests: first using the traditional (telephone) and then using a mobile application. The experiment will be discussed further in Chapter 3.

SeeClickFix has already developed a mobile application that collects work requests for government infrastructure. April Joyner (2010) published an article titled "For Making it Easy to be a Good Citizen". In the article, she stated, that SeeClickFix has collected "more than 65,000 reports of problems from residents in 10,000 communities" (p. 100). The creator of the application, Ben Berkowitz, initially created it for his home town in New Haven, Connecticut, but it is now being used all over the United States (Joyner, 2010).

Hilton Collins (2011) reported in an article, titled "Fixing by Clicking", that "Berkowitz said, 'You can save money by getting citizens to report issues to governments [rather than] paying people to go out and inspect the public space…opposed to reporting issues over the phone'" (p. 27). The application makes it possible for anyone with an appropriate (Android, Windows, or iOS) internet-connected mobile device to report infrastructure deficiencies. It also collects, organizes, and communicates public works issues between citizens and government entities (Collins, 2011).

Several things happen when a user submits a work request via the application. The location of the issue is recorded using GPS technology and a notification is sent to the appropriate public works department. Furthermore, the user can upload photos of the issue, receive notifications about the status of the issue, and add written details about the issue (Collins, 2011).

SeeClickFix is customizable to a specific location (Collins, 2011). Therefore, it has potential to increase the effectiveness of the CE mission to sustain installations. Theoretically, anyone with a phone and access to a base would be able to snap a picture and submit work requests to CE via the application interface. Using the SeeClickFix application (or one like it) would allow CE customer service to communicate back-and-forth with their customers and every member of the base populace would become a sensor for infrastructure issues. However, this research does not intend to prove the effectiveness of the application but rather investigate the question about operational security using an OPSEC approach.

Media Richness Theory

Different forms of communication, or communication mediums have varying degrees of richness. According to Daft and Lengel (1986), "information richness is defined as the ability of information to change understanding within a time interval" (p. 560). The "richer" the communication medium, the more effective it is at changing understanding. For example, Daft and Lengel (1986) rank face-to-face communication higher in richness that a written documents because it provides immediate feedback via body language and tone of voice. Figure 3 is a visual display of how Lengel and Daft (1988) rank communication mediums.

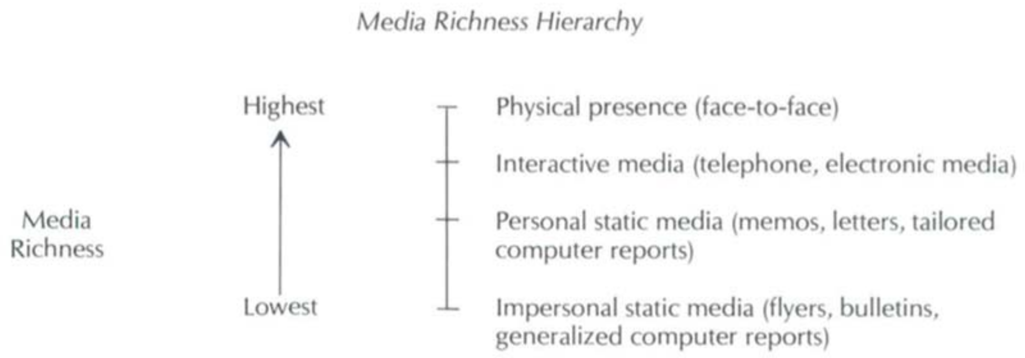

Media Richness Hierarchy
Highest
Lowest
Media Richness
Physical presence (face-to-face)
Interactive media (telephone, electronic media)
Personal static media (memos, letters, tailored computer reports)
Impersonal static media (flyers, bulletins, generalized computer reports)

Figure 3. Media Richness Hierarchy (Lengel and Daft, 1988)

According to Lengel and Daft (1988), “the more learning that can be pumped through a medium, the richer the medium” (p. 226). This means that the communication medium chosen is more effective when the intended audience learns the most about the information being communicated. Furthermore, Lengel and Daft (1988) rank “richness” of a medium based on the existence of the following characteristics:

1. Ability to handle multiple information cues simultaneously
2. Ability to facilitate rapid feedback
3. Ability to establish a personal focus

The effectiveness of the communication depends on the medium selected. For this reason, Lengel and Draft (1988) divided communication into two categories, routine and non-routine communication. They suggest that a rich medium is required for non-routine communication and a leaner medium is appropriate for routine communication. For example, if a manager wants to motivate their employees, it would be better to personally visit them rather than send a corporate email (Lengel & Draft, 1988). According to Lengel and Draft (1988), a “face-to-face medium…convey[s] the human side of the executive and the cues of personal interest, caring, and trust that are filtered out of a written medium" (p. 230). Therefore, the use of a richer medium will increase the effectiveness of communication.

The experiment conducted in this research had participants report infrastructure deficiencies using two different methods (telephone and mobile application). Based on the media richness theory, the mobile application was considered to be a "richer" form of communication because it includes written and visual (pictures or electronic media) communication methods versus only a verbal telephone conversation.

Critical Information

Table 3 is a list of critical information categories that summarizes over 200 examples of critical information found during the review of literature. The majority of the examples can be found in JP 3-13.3 (2006). However, examples from other service specific documents, such as AFI 10-701 (2011), were used to derive the 10 critical information categories. Table 3 is a product of this review of literature and was used to pre-identify critical information within the experimental scenarios. A positive event occurred when the pre-identified information was captured and communicated to a simulated CE customer service.

Table 3. Critical Information Categories

#	Critical Information Categories
1	Military Capabilities, Limitations and Intentions
2	Logistic Capabilities and Limitations
3	Alert Posture
4	Forces/Assets Assigned, Movement, and Location
5	Communications (Methods, Capabilities and Limitations)
6	Administration, Finance, and Personnel
7	Procedures
8	Infrastructure (Locations, Condition, Construction and Maintenance)
9	Security Capabilities and Limitations
10	Research Development, Acquisitions Contracts and Technologies

Hypothesis

Based on the media richness theory, a mobile application is consider a "richer" communication medium. Therefore, the following hypothesis was derived based on a review of the OPSEC process, the WRCP, and the media richness theory:

> **Hypothesis**: A mobile application will collect more critical information than the traditional call-in method of submitting a work request.

Where the *amount of critical information collected* is the dependent variable and the *collection method* is the independent variable. The experiment developed in Chapter 3 will test this hypothesis.

Conclusion

This chapter covered how to measure security risks using the five-step OPSEC process, described the WRCP, elaborated on the media richness theory and introduced the SeeClickFix mobile application. Based on this review of literature, a list of critical information categories (Table 3) was developed and a research hypothesis was derived.

This research evaluates the OPSEC risks associated with integrating a mobile application into a CE workflow process. It is the first academic study of its kind. Based on this author's knowledge and best efforts to find relevant research, there is not any current published sources that show an actual implementation of the OPSEC process with regards to WRCP—nor is there any research that uses an experimental design to evaluate OPSEC risks associated with a WRCP.

III. Methodology

Introduction

In Chapter 2, examples of critical information and indicators (CII) of critical information were identified and summarized into 10 categories (Table 3). This chapter will describe the theory, resources, and processes used to design the experiment, collect data, and analyze the results. The purpose of this research is to identify and evaluate OPSEC risks associated with the collection of infrastructure deficiency data. This was done by gathering and analyzing experimental data to answer the following question: *Does using a mobile application to collect work requests increase, decrease, or have a null effect on OPSEC?* Answering the research question will help Air Force leaders make an informed decision about the utilization of a mobile application to collect work order data.

Theory

Design of Experiments (DOE)

In the article titled "Keys to Successful Designed Experiments," Mark Anderson and Shari Kraber (2002) identified "eight keys to success in applying statistical tools for design of experiments" (p. 1). The keys for success were carefully considered during the design of the experiment that is described in this chapter. The "eight keys" are provided in Table 4.

Table 4. Keys to Successful Design of Experiments (Anderson & Kraber, 1999)

#	Keys to Success
1	Set good objectives
2	Measure responses quantitatively
3	Replicate to dampen uncontrollable variation
4	Randomize the run order
5	Block out known sources of variation
6	Know which effects (if any) will be aliased
7	Do a sequential series of experiments
8	Always confirm critical findings

Hypothesis Testing

During the experiment, human subjects used one of two methods of submitting work requests to a simulated Civil Engineer Squadron. Half of the subjects used a mobile application to submit requests and the other half used the traditional call-in method to submit the same requests. Therefore, the two samples include the amount of CII collected using the traditional versus application collection method. Where the number of CII collected was the response variable. Hypothesis testing was used to analysis the statistical difference of the response of the two separate collection methods.

According to Mildred L. Patten (2009), author of the book *Understanding Research Methods: An Overview of Essentials*, there are three explanations for differences between randomly sampled data sets (p. 105). The three explanations are: (1) the difference is an accurate representation of the population, (2) there is bias in the procedures, (3) the samples do not represent the population because of random sampling error (Patten 2009). Hypothesis testing is used to address the third explanation.

For this research, hypothesis testing was used to determine if the difference between the amount of CII collected by the mobile application and the traditional process was statistically significant. The research hypothesis is:

Hypothesis: A mobile application will collect more critical information than the traditional call-in method of submitting a work request.

Where the *amount of critical information collected* is the dependent variable and the *collection method* is the independent variable.

Human Subjects and Equipment

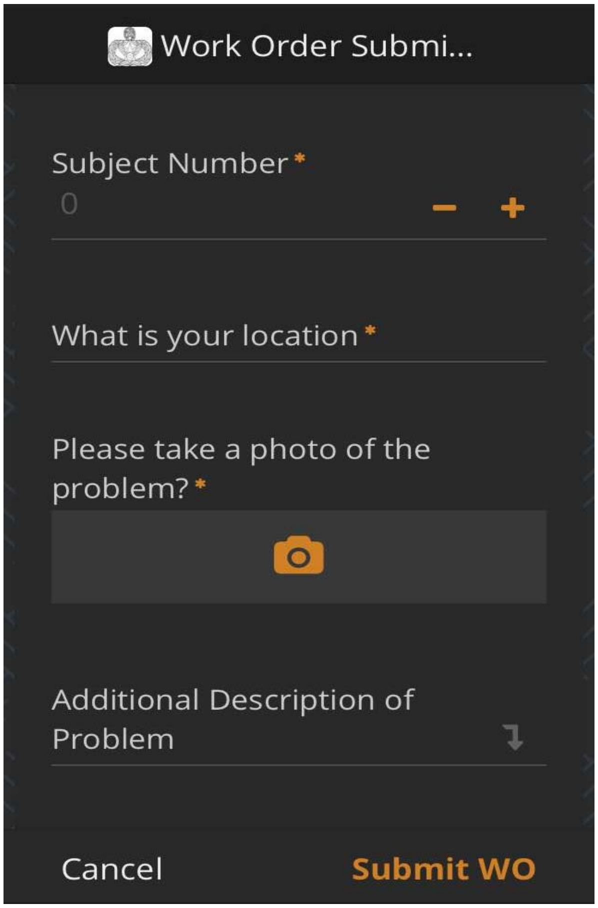
The IRB Process

This research used human subjects to collect work order data. Therefore, the experiment was subject to approval by an Institutional Review Board (IRB) prior to data collection. The request was reviewed and approved by the Air Force Research Lab IRB. As required by the IRB, an informed consent form (ICF) was provided to each subject. Every subject read and signed the informed consent prior to participating in this research.

The ICF was provided to each participant prior to participating in the study and a standardized script was read to each participant. A copy of the approved ICF is located in Appendix 1 and the script is located in Appendix 2. The purpose of the ICF was to make each subject aware of the purpose of the study, potential risks, benefits, costs, compensation, confidentiality, and the completely voluntary participation policy. Whereas, the script ensured each subject was given identical instruction and helped avoid potential variation or bias by standardizing experimental instructions. Like the ICF, the script was also required by the IRB.

Mobile Application

The mobile application used during the experiment was created using an online program called AppSheet. Human subjects used the mobile application, titled the "Work Order Submission Application", to report infrastructure problems that were pre-determined along a set course. The subjects reported the issue by filling out the fields located on the application interface (see Figure 4). This included the subject number, location of the issue, a photo of the problem, and any additional information needed to describe the problem.



Work Order Submi...

Subject Number *
0

What is your location *

Please take a photo of the problem? *

Additional Description of Problem

Figure 4. Mobile Application Interface

Call-in Method

A mobile phone was used (by subjects) to collect infrastructure problems using a call-in method. The call-in method simulated the traditional method of calling in a work request to CE customer service. Subjects using the traditional call-in method called a number that linked directly to a Google Voice mailbox. Then the voicemail recording would ask the subject to record, “their subject number”, “their location”, and “a description of the infrastructure problem they were trying to submit”. After the tone the subjects were asked to leave a message that included the previous details.

The voicemail recording was used to collect the data because this technique ensured standardization of the questions being asked and avoided the potential for recording errors. For example, if a human had received the phone call it would have been possible for them to misspeak while asking the questions or misinterpret and improperly record the response. Furthermore, the voicemail recording was replayable and had a speech-to-text feature that simplified the documentation of the data collected.

Post Experiment Questionnaire

The purpose of the post-experiment questionnaire was to collect subject demographics (e.g. age, gender, job title…etc) and some additional information questions used to assess subject bias and familiarity with OPSEC. Therefore, in addition to the primary purpose of this research, the questionnaire enabled the researcher to investigate possible relationships between the participant’s personal characteristics (OPSEC training experience, pay grade, age, and job type) and whether or not they collected CII.

In order to avoid bias, the participants were not told that they could be capturing CII. However, they were asked, via the questionnaire, whether or not they considered

OPSEC during the experiment and how familiar they were with the meaning of OPSEC. Furthermore, the participants were asked if they knew that the study was about OPSEC prior to participating. This was an important question, because if the participants knew they were collecting OPSEC, they may or may not have intentionally avoided collecting CII. A full copy of the post-experiment questionnaire can be found in Appendix 3.

Procedures and Processes

Identifying Infrastructure Problems for the Experiment

In order to increase the validity of this study, a method was needed to logically determine what type of work requests should be submitted during the experiment so as to replicate real-world facility issues as much as possible. Therefore, a trend analysis was conducted on "real data" to identify trending work requests. A two-year sample of work orders from Dover Air Force Base (AFB) was acquired from the interim work information management system (IWIMS). The data was used to identify frequently reported work orders and the CE repair shop responsible for those types of work orders.

Only direct schedule work (DSW) type work orders were considered. Direct scheduled work orders are minor modifications to infrastructure that do not require a large amount of time, money, or manpower to complete (Davis, 2013). DSW type requests were used because this research assumes that the mobile application would be used to collect similar type of work orders. For example, customer would be submitting issues such as potholes and water leaks rather than a request for a building renovation or new facility construction. Major work requests would still require a more detailed traditional submission process that is not covered in this research.

A trend analysis was conducted on the sample of work orders from Dover AFB. First, the data was divided into individual repair shops and a count was conducted to determine which shops had the majority of the work orders (see Figure 5). Figure 5 clearly indicates that the majority of work orders are related to Structures, Heating Ventilation and Air Conditioning (HVAC), Water, and Electrical.

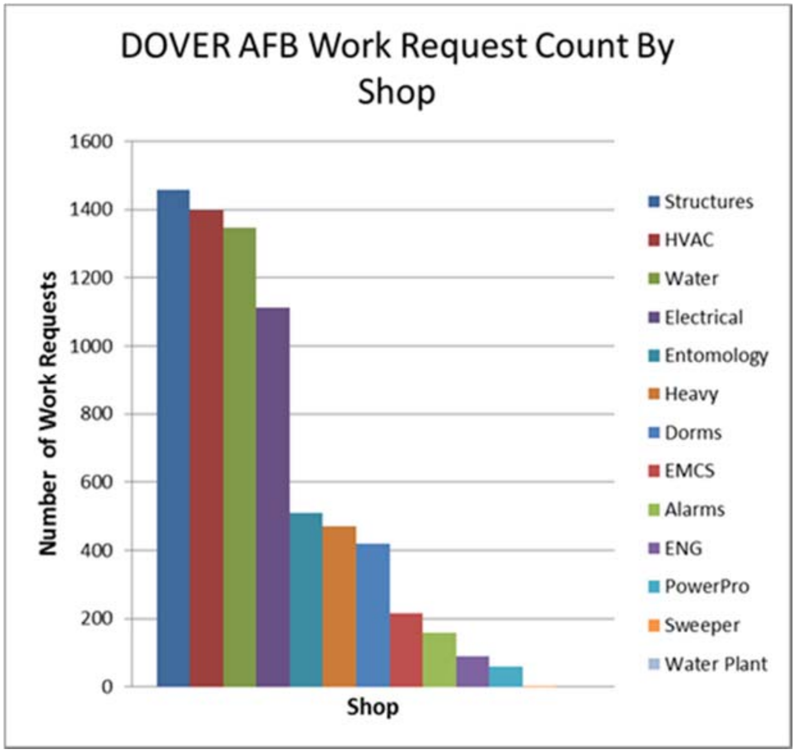


Figure 5. Work Order Distribution by Shop (Dover AFB)

Next, a custom word-cloud generator was programmed in R. The *work order description field* from the entire list of work orders (separated by shop) was input into the cloud generator to determine what words were most frequently used. The program removed common English "stopwords" (e.g. a, the, this, etc) and frequent but useless words (e.g. repair, replace, broken, etc) were removed. See Figure 5 for an example of the word cloud used to identify common types of work requests. Figure 5 clearly depicts that the most common issues (based on a two year history) for the electrical shop at Dover AFB, are lights.

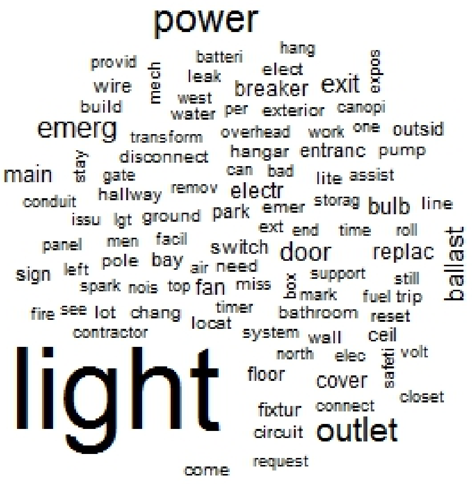
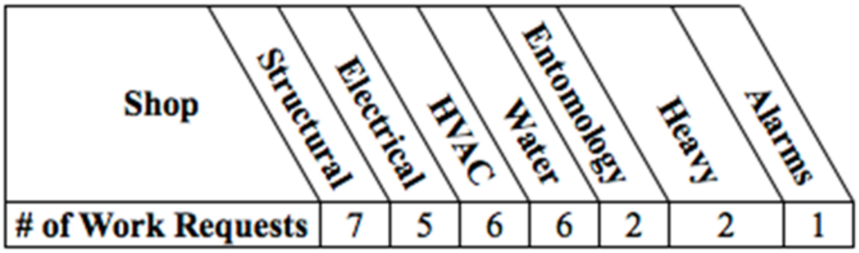


Figure 6. Word Cloud - Electrical Shop Work Order Description (Dover AFB)

The process described above identified the most frequent type of DSW orders submitted to CE customer service from July 2014 through July 2016 at Dover AFB. Common issues were identified using historical data. A walk through the Air Force Institute of Technology (AFIT) campus (experiment location) was conducted and 29 infrastructure deficiencies were identified. The 29 issues were chosen by comparing the results of the word cloud to real issues identified during the walk-around or an issue was simulated (e.g. overflowing sink) to capture a realistic distribution of common work requests. See Appendix 4 for a list of the deficiencies identified during the walk through. The distribution of work requests was evenly spread across 7 shops based on the relative percentage of total work orders actually identified at Dover AFB. Table 5 shows how the work requests were distributed by shop (compare to Figure 5).

Table 5. Distribution of Work Requests by Shop



Shop	Structural	Electrical	HVAC	Water	Entomology	Heavy	Alarms
# of Work Requests	7	5	6	6	2	2	1

Designing the Experiment

The experiment was designed while considering Anderson and Kraber's (2002) "eight keys to success in applying statistical tools for design of experiments [DOE]" (p. 1). The first key is "Set Good Objectives" and is focused on optimizing the critical aspects of the experimental process and eliminating non-critical elements (Anderson & Kraber, 2002). The purpose of this research is to identify and evaluate OPSEC risks associated with the collection of work order data. This was done by gathering and analyzing empirical data to answer the following question: *Does using a mobile application to collect works requests increase, decrease, or have a null effect on OPSEC?*

The critical experimental process that was emphasized during the experiment was the collection of CII. Therefore, each of the 29 locations was evaluated and CII at each location were pre-identified. Appendix 5, *Researcher's Grading Rubric*, is a list of all CII pre-identified at each location and a rubric used by the researcher to consistently and accurately count the number of CII (response variable) captured by each subject at each of the 29 locations. Table 6 is a partial list and provide here as an example of CIIs that were pre-identified. The category column of Table 6 is the associated CII category from Table 3.

Table 6. List of Pre-identified CII

Potential CII	Category
Identification of Personnel	#6 - Administration, Finance, and Personnel
Location of Comm. Equipment	#5 - Communications (Methods, Capabilities and Limitations)
Building Map	#8 - Infrastructure (Locations, Condition, Construction and Maintenance)
Increased Access Security	#9 - Security Capabilities and Limitations

The pre-identified list of CII was used to quantify the response by comparing the data collected and determining if CII was reported. This was the objective of the experiment and satisfied the first "key to success" (Anderson & Kraber, 2002). The second key is "Measure Responses Quantitatively" (Anderson & Kraber, 2002). For this study, the response was the collection of CII. Therefore, at each of the 29 location participants would submit a work request. After the subjects submitted the work requests, the number of CII captured was counted using the *Researcher's Grading Rubric* (Appendix 5) as a guide to consistent measurement.

For example, the location of communication equipment was pre-identified as CII under category 5 of Table 3, *Critical Information Categories*. If a subject reported the location of a communications closet via the application or call-in method it was counted as positive event. Multiple events at the same location were summed together. Therefore, the response (number of CII reported) was measured quantitatively.

The third key is "Replicate to Dampen Uncontrollable Variation (Noise)" (Anderson & Kraber, 2002). Each participant was given the exact same training before starting the experiment. The script (Appendix 2) includes the standardized training that was provided to each participant. Standardized training was performed in order to avoid a potential source of variation. However, each participant has different levels of knowledge and abilities that are difficult to measure. Therefore a goal of sixty participants was established in the hopes of overcoming any noise variation that would be encountered and to obtain adequate power. According to Jacob Cohen (1992), a larger sample size increases the desired "power desired" (p. 156). A snowball sampling method was used to randomly select participants.

The fourth key is "Randomize the Run Order" (Anderson & Kraber, 2002). Randomization was built into the experiment in two ways. Each participant was randomly assigned a direction and method (application or traditional). The random direction means the participant would either start at location 29 working toward location one or vice versa. The method was assigned randomly so that there would be an equal number of participants submitting via the application or traditional call-in method. Therefore, each participant either used the app method or the call-in method, but never both.

The fifth key is " Block Out Known Sources of Variation" (Anderson & Kraber, 2002). The most known source of potential variation was the subject knowing about potential OPSEC before participating in the experiment. Therefore the entire purpose of the study was not revealed until after the study. However, some participants may have been unintentionally biased based on their proximity to the researcher and the research study location (e.g. student's at AFIT). Therefore, each participant had the opportunity to self-identify any previous knowledge while taking the post-experiment questionnaire.

Also, it was asked that the participants not talk to anyone about the study until after the results were published.

During the data collection phase, the researchers would only answer questions that were intended to clarify the instructions given on how to report the infrastructure deficiency. That way every subject received the same information about the description and location of the infrastructure problem they were reporting. Furthermore, as the subjects were reporting the problem, the researchers stood in the same location during each run of the experiment. The position of the researcher was considered important, because depending on where they were standing, it was possible to for the researcher to obstruct the view of a CII that may otherwise have been reported. Standardized instructions via the initial reading of the script (Appendix 2), phrases used to identify the issue, and the standing position of the researchers were all regulated to reduce possible know sources of variation during the experiment.

The sixth key is "Know Which Effects (if any) will be Aliased" (Anderson & Kraber, 2002). This topic referrers to changing more than one variable at a time and identifying sources of interaction between variables (Anderson & Kraber, 2002). There is only one intended change within each run of the experiment (other than randomization) and that is the collection method. However, while the majority of the subjects were military members that have been trained on OPSEC, some of the subjects had no training at all. There is no way to completely standardize the human subjects. Therefore, each subjects demographic information was collected using the post-experiment questionnaire (Appendix 3) and was used to compare results between subject in the next chapter.

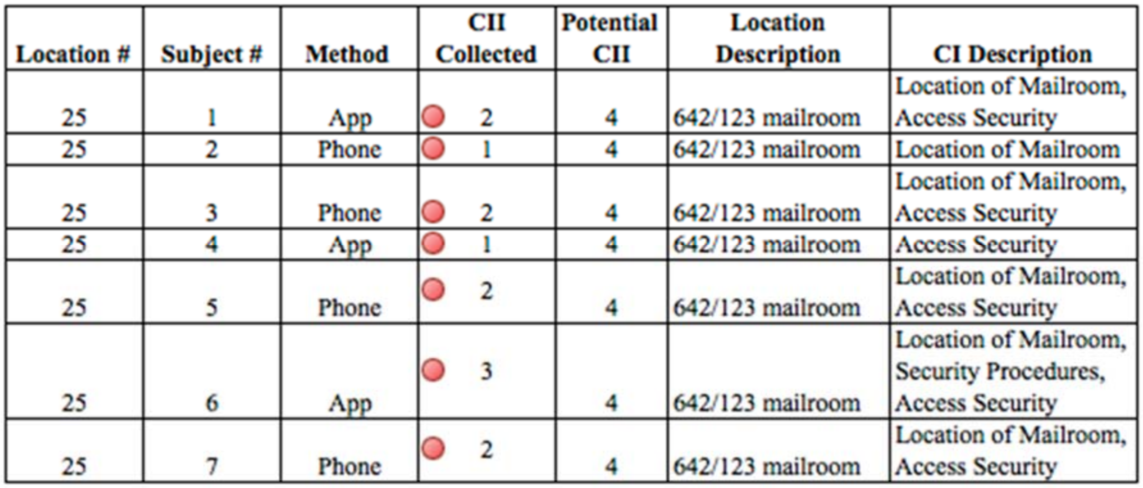
The seventh key is “Do a Sequential Series of Experiments” (Anderson & Kraber, 2002). This means performing the experiment in sequential steps in order to apply lessons learned to future runs of the experiment (Anderson & Kraber, 2002). A pilot study was conducted with four participants. The primary lesson learned from the pilot study was that there needed to be a question about the subject’s prior knowledge of the experiment’s purpose on the post-experiment questionnaire. Additionally, any variation caused by the standing location of the researchers to standardized instructions, were solidified during the pilot study and the results of those four participates were compared to the results of other participants in Chapter 4.

Anderson and Kraber’s (2002) “eight keys to success in applying statistical tools for design of experiments” were used to guide the experimental design (p. 1). Reducing variation, researcher bias, and subject bias was considered critical during the DOE and data collection process. The eighth key, “Always Confirm Critical Findings” was implement in subsequent chapters by re-running statistical analysis and comparing the results of two separate statistical test.

Recording the Data

Data was recorded differently for each data collection method (application and traditional). However, the data was all consolidated into one data file. The response was the total number of CII collected at each location by each subject. Table 7 is an example of the final consolidated data file excluding a few columns (e.g. grouping variables, normalization, etc) that were removed to allow fit the table to this document.

Table 7. Sample of Consolidated Results



Location #	Subject #	Method	CII Collected	Potential CII	Location Description	CI Description
25	1	App	● 2	4	642/123 mailroom	Location of Mailroom, Access Security
25	2	Phone	● 1	4	642/123 mailroom	Location of Mailroom
25	3	Phone	● 2	4	642/123 mailroom	Location of Mailroom, Access Security
25	4	App	● 1	4	642/123 mailroom	Access Security
25	5	Phone	● 2	4	642/123 mailroom	Location of Mailroom, Access Security
25	6	App	● 3	4	642/123 mailroom	Location of Mailroom, Security Procedures, Access Security
25	7	Phone	● 2	4	642/123 mailroom	Location of Mailroom, Access Security

For the application method, the user input the data using the mobile application interface, and the application saved the information (including pictures) to a Google Drive location. The data collected using the call-in method consisted of a voice recording that was transcribed by Google Voice to a written transcript. After all the data was collected, the researcher manually identified CII that was captured at each location using the *Researcher's Grading Rubric* (Appendix 5). This consisted of listening to each recording, reviewing every picture, and looking at every piece of data that was submitted by each subject.

Summary

This chapter outlined the procedures and methods used to perform hypothesis testing, comply with IRB requirements, identify the work request and locations, design the experiment, and collect and record the data. The purpose of this study is to answer the following question: *Does using a mobile application to collect work requests increase, decrease, or have a null effect on OPSEC?* Specifically the experiment measured the amount of information (CII) that was communicated to a simulated CE customer service section. The prior identification of CII at each location was performed to identify potential OPSEC vulnerabilities. However, the purpose of this experiment was not to debate whether or not the information collected was “actually” CII.

Each unit in the Air Force is responsible for identifying CII that is pertinent to their specific mission objectives. When the researcher identified potential CII, it was assumed that an adversary had the appropriate resources, desire, and motivation to obtain the information (e.g. hacking the telephone conversation or application data). It was not feasible to include specific CII for every unit in the Air Force. Therefore the researcher identified CII that corresponded to the locations that were identified by common types of DSW work requests. The research question will be answered based on whether or not the mobile application (considered a richer medium) communicated more pre-identified information than the traditional call-in method. The next chapter will discuss statistical analysis and results.

IV. Analysis and Results

Overview

In this chapter the results of the experiment and the analysis of those results will be presented. There were a total of 40 participants that took part in the experiment. Half of the participants went through the experiment submitting work requests using the mobile application and the other half submitted the same requests using the traditional call-in method. After participating in the study, each subject completed a post-experiment questionnaire (Appendix 3).

Table 8 shows a summary of the demographics that each subject reported on the post-experiment questionnaire. The average age of the 40 participants was 28 years old and half of those participants were from the Civil Engineer career field. Furthermore, most (90%) of the participants were male and all the participants had obtained at least a bachelor's degree at the time the experiment was conducted. The majority (83%) of the subjects were company grade officers (CGOs).

Table 8. Subject Demographics

Age (years)	*Range:* 23-45 *Mean:* 28 years old
Career Field	*Civil Engineer:* 20 *Other:* 20
Gender	*Male:* 36 *Female:* 4
Education	*Bachelor's:* 34 *Master's:* 6
Rank	*CGOs:* 33 *Civilian:* 4 *FGOs:* 2 *Enlisted:* 1

Results of Pilot Study

Prior to starting the experiment, four subjects participated in a pilot study. The purpose of the pilot study was to test the experimental design and identify any sources of variation prior to continuing. There were two changes made to the experiment after the pilot study was conducted. First, the researchers conducting the experiment standardized their standing location while the each subject was submitting work requests. Standing location was considered important because it was possible for the researcher to stand in a location that blocked the participant's view to CII. Second, a question was added to the post-experiment questionnaire that allowed participants to identify whether or not they were previously aware that the study was investigating OPSEC.

The question was added to identify potential subject bias. If the subject was aware of the research purpose prior to participating it was possible that the participant would respond differently. The main concern was that subjects with prior knowledge about the study might be more likely to identify CII during the experiment and intentionally avoid collecting it. Therefore, the responses (total number of CII collected) of participant with prior knowledge about the study were averaged and compared to the average responses of participants that did not have any prior knowledge.

Table 9 shows the results of the comparison. There was a total of 655 CIIs collected by all 40 subjects during experiment and six of the 40 participants self-identified as having prior knowledge about the purpose of this research. Out of those six, only two of the subjects used the application method and the other four used the call-in (phone) method. As shown in Table 9, the mean comparison does show that subjects with prior knowledge collected (on average) a lower percentage of CII. In order to determine if the 6 participates had an impact on the overall results they were removed from the data after the initial hypothesis testing was conducted and the tests were re-accomplished. The results will be discussed in more detail later in this chapter. However, they did not have an impact on the overall results and conclusion of this study.

Table 9. Mean Comparison of Subjects With Prior Knowledge of Study Vs. Subjects Without Prior Knowledge

	Prior Knowledge	No Prior Knowledge
Phone	*Mean:* 49/4 = 12.25%	*Mean:* 212/16 = 13.25%
Application	*Mean:* 23/2 = 11.5%	*Mean:* 371/18 = 20.61%

Hypothesis Testing

Hypothesis testing was used to determine whether or not the application collected more CII than the traditional call-in method. Therefore, the results were divided into two groups. The first group included the responses (number of CII collected) for the subjects who used the mobile application and the second group included responses for the subjects who used the traditional method. Since there were only two groups, a *Student's t-test* was considered the appropriate statistical method of comparing the means of the two groups. However, in order to use the *Student's t-test*, each group would have to satisfy the assumption of normality.

The statistical analysis was conducted using R. Before any of the tests were run, the response variable was normalized by dividing the actual number of CII collected by the pre-identified potential CII value for each location. Therefore the response variable was normalized to a scale from 0 to 1. This was necessary due to the fact the number of pre-identified CII varied from a minimum of one to a maximum of five between each location. After the response was normalized each group was tested for normality. All the statistical tests in this analysis were conducted using a confidence coefficient (alpha) of .05.

Test for Normality

The Shaprio-Wilk test was performed for each group and each group failed the assumption of normality. The null hypothesis for the Shaprio-Wilk test is that the response is normally distributed. The first group tested was the numerical response (amount of CII collected) of the mobile application. The test result (S-W = .78, df = 580, p < .001) for the first group indicated that the assumption of normality did not hold and the response is not normally distributed. This was the same for the test of normality for the response of the second group or the response associated with the traditional method (S-W = .68, df = 580, p < .001).

In addition to the Shaprio-Wilk test, a quantile-quantile (QQ) plot created and the skewness and kurtosis values were observed. The QQ plot was used to visually inspect the two groups for the assumption of normality. For the assumption of normality to hold, the response should follow a linear pattern. However, the results of the QQ-plot for both groups (Figure 7) show a non-linear trend. Furthermore, Table X shows the skewness and kurtosis values for each group. For both groups the skewness values were above 1. This indicates that the distributions data is highly skewed to the right. The results of the A Shaprio-Wilk test, the visual inspection of the QQ plot, and the high skewness values all indicate the response data is not normally distributed.

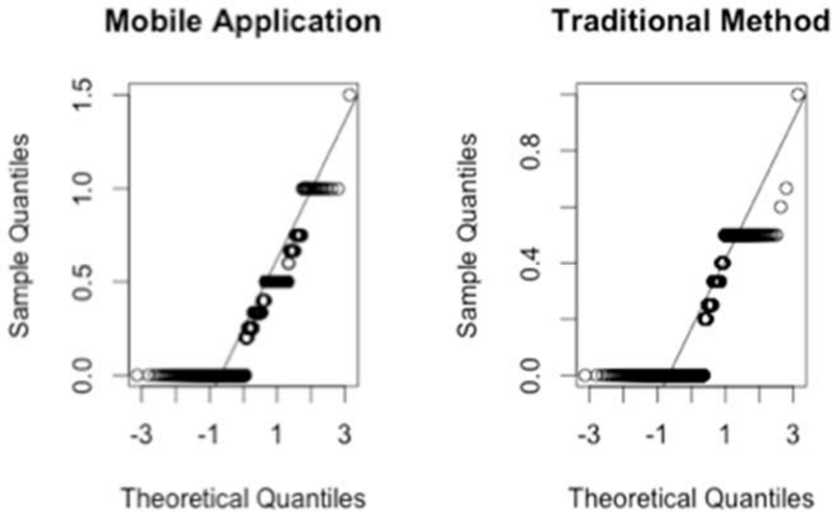


Figure 7. QQ-Plots

Table 10. Skewness and Kurtosis Values

	Skewness	Kurtosis
App	1.03	0.308
Phone	1.01	-0.406

The normality assumption of the Student's t-test was not satisfied. Therefore, a non-parametric analysis was performed instead. The *Wilcox Rank-Sum Test* was the non-parametric hypothesis test used to compare the two groups because it does not require normality or equal variance. A one-sided Wilcox Test (WT) was conducted by comparing the medians of both groups, Group A and Group B. Where, for the first test, Group A is the response variable of the mobile application collection method and Group B is the response of the traditional method.

The null hypothesis (H_0) for the first WT conducted is that the median difference between the two groups is zero and the alternate hypothesis (H_A) for a one-side test is that the median for Group A is greater-than the median of Group B. Therefore, if the resulting p-value is less than .05 the null hypothesis is rejected in favor of the alternate. For this "overall" test, the results (*Z* = -5.18, *p* < .001) indicated that the application collected more CII than the traditional method at a 95 percent level of confidence. Thus confirming the study hypothesis first introduced in Chapter 2—a mobile application will collect more critical information than the traditional call-in method of submitting a work request.

Hypothesis Testing: Grouped by Location

The previous results were based on the overall CII collected (response) by each collection method independent of the actual location. The next series of WTs evaluated each of the 29 locations separately. Where Group A is the response of the mobile application at each location and Group B is the response of the traditional method at each separate location.

The results of the WTs are tabulated in Table 11. Where H_O is the null hypothesis of the WT, H_A is the alternate, and M represents the median. A p-value highlighted in red indicates that the level of significance was below the confidence coefficient (.05). In those cases, the null hypothesis was rejected for the alternate. For example, the results for location 1 are located on the first row of Table 11. These are the results of two different one-sided WTs. The results of the first test (H_A: $M_A > M_B$, *Z* = -3.69, *p* < .001) indicate that the application collected more CII than the traditional method. Likewise, when the one-sided test is reversed (H_A: $M_A > M_B$) the results of location number 13 (*Z* = -2.03, *p* < .001) show that the traditional method collected more CII than the application.

The results of grouping by location (Table 11) shows that 9 out of the 29 locations had the application collecting more CII that the traditional method, 1 of the 29 locations resulted in the phone collecting more CI, and the remaining 19 locations shows no statistical difference between the application and the traditional method. These results will be further discussed in the next chapter.

Table 11. Results of the Wilcox Rank-Sum Test Grouped by Location

Location #	**H_O: M_A-M_B = 0 H_A: M_A > MB**	**H_O: M_A-M_B = 0 H_A: M_A < MB**	**Result**
1	$Z = -3.69$, $p < .001$	$Z = 0$, $p = 1$	App Collected More CII
2	$Z = 0$, $p = 1$	$Z = 0$, $p = 1$	No Difference
3	$Z = -4.59$, $p < .001$	$Z = 0$, $p < 1$	App Collected More CII
4	$Z = -2.58$, $p = .001$	$Z = -.011$, $p = .991$	App Collected More CII
5	$Z = -1.29$, $p = .198$	$Z = -.240$, $p = .810$	No Difference
6	$Z = 0$, $p = 1$	$Z = 0$, $p = 1$	No Difference
7	$Z = -1.14$, $p = .253$	$Z = -.309$, $p = .758$	No Difference
8	$Z = -.973$, $p = .330$	$Z = -.412$, $p = .681$	No Difference
9	$Z = -2.57$, $p = .010$	$Z = -.011$, $p = .991$	App Collected More CII
10	$Z = -.302$, $p = .762$	$Z = -1.16$, $p = .247$	No Difference
11	$Z = 0$, $p = 1$	$Z = 0$, $p = 1$	No Difference
12	$Z = -.089$, $p = .929$	$Z = -1.74$, $p = .081$	No Difference
13	$Z = -.048$, $p = .962$	$Z = -2.03$, $p = .042$	Phone Collected More CII
14	$Z = -4.59$, $p < .001$	$Z = 0$, $p = 1$	App Collected More CII
15	$Z = -1.74$, $p = .081$	$Z = -.089$, $p = .929$	No Difference
16	$Z = -1.74$, $p = .081$	$Z = -.089$, $p = .929$	No Difference
17	$Z = -2.76$, $p = .005$	$Z = -.007$, $p = .995$	App Collected More CII
18	$Z = -1.37$, $p = .171$	$Z = -.185$, $p = .853$	No Difference
19	$Z = 0$, $p = 1$	$Z = 0$, $p = 1$	No Difference
20	$Z = -1.74$, $p = .081$	$Z = -.089$, $p = .929$	No Difference
21	$Z = -0$, $p = 1$	$Z = 0$, $p = 1$	No Difference
22	$Z = -2.05$, $p = .040$	$Z = -.044$, $p = .965$	App Collected More CII
23	$Z = -4.37$, $p < .001$	$Z = 0$, $p = 1$	App Collected More CII
24	$Z = -.744$, $p = .457$	$Z = .582$, $p = .561$	No Difference
25	$Z = -4.70$, $p < .001$	$Z = 0$, $p = 1$	App Collected More CII
26	$Z = -1.30$, $p = .192$	$Z = .232$, $p = .816$	No Difference
27	$Z = -.997$, $p = .319$	$Z = .396$, $p = .692$	No Difference
28	$Z = -.572$, $p = 567$	$Z = .764$, $p = .445$	No Difference
29	$Z = -.935$, $p = .350$	$Z = .438$, $p = .661$	No Difference

Hypothesis Testing: Grouping Locations With High and Low Potential CII

Another way the results were analyzed was by grouping locations with "high" and "low" potential CII. This grouping method investigated whether or not the amount of potential CII available had any impact on the results. Therefore, based on the chart in Figure 8, a location was considered having high potential CII if the pre-identified amount of CII was equal to or greater than 3 (red bars). Likewise, the location was considered low if there were less than 3 potential CIIs available (blue bars).

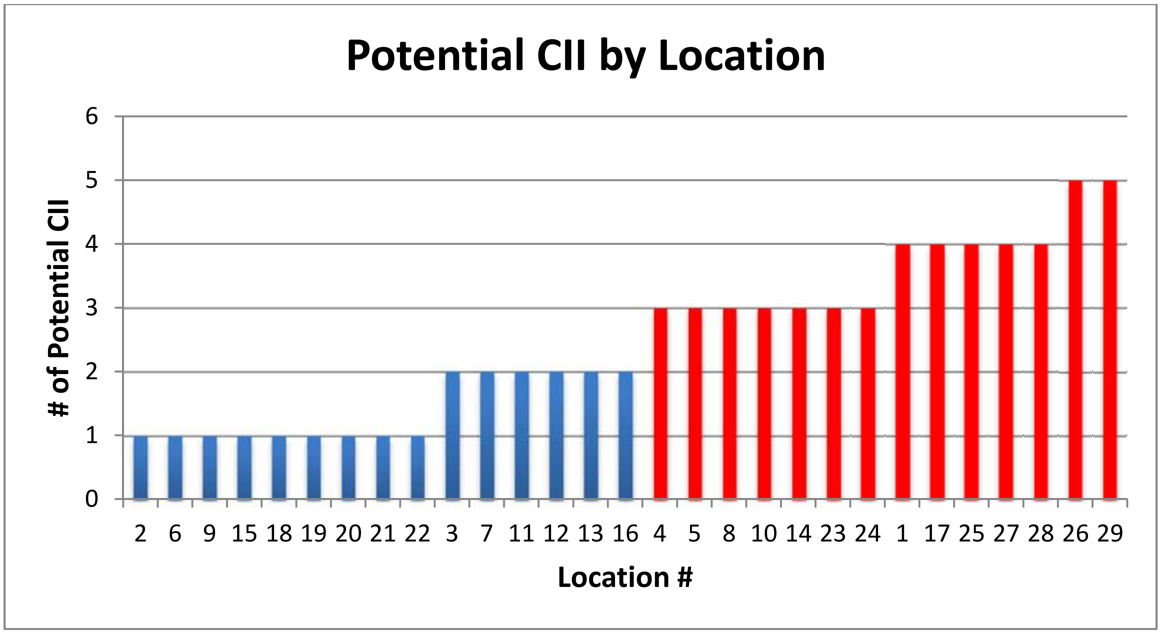


Figure 8. Potential CII by Location

Two WTs were performed for this grouping technique. For both tests, Group A was the response of the mobile application and Group B was the response of the traditional method. However, the first test compared the responses for locations that had low CII and the second compared locations with high CII based on Figure 8. The results of both tests are shown in Table 12.

Table 12. Results of the WT for Grouping by High and Low Potential CII Locations

Group	**H_O: M_A-M_B = 0** **H_A: M_A > MB**	**Sample Size**	**Result**
Low	Z = -2.94, p = .003	n_A = 300, n_B = 300	App Collected More CI
High	Z = -4.88, p < .001	n_A = 280, n_B = 280	App Collected More CI

A one-sided test was performed to determine if the application collected more CII than the traditional method. For grouping by high and low potential CII, the application method collected more CII. This provides evidence to conclude that regardless of how much CII was available at the experiment locations—the application still collected more CII at great-than a 95 percent level of confidence.

Hypothesis Testing: Grouping by Air Force Specialty Code (AFSC)

Another way the results were grouped and analyzed was by the subject's AFSC. Twenty of the 40 participants were part of the Civil Engineer (CE) career field (AFSC: 32E) and the other 20 were either civilian or from another Air Force career field. Therefore, it was assumed that the CE subjects were more familiar with reporting infrastructure deficiencies than the "other" subjects. Therefore, this test was performed to investigate whether or not CE subjects had any impact on the outcome. For example, if the CE subjects were more familiar with reporting infrastructure problems they may be more likely to communicate additional information. Reporting more information could lead to capturing a greater amount of CII.

Similar to the previous sections, a WT was preformed to see if CE and "other" subjects captured more CII using the application. However, this time the responses were grouped by AFSC. Table 13 shows the test results. Where the sample was divided evenly with 10 participates using the app and 10 using the call-in method for both groups.

Table 13. Results of Wilcox Ranked-Sum Test for Grouping by AFSC

AFSC	**H_O: M_A-M_B = 0** **H_A: M_A > MB**	**Sample Size**	**Result**
32E	Z = -5.31, p < .001	n_A = 290, n_B = 290	App Collected More CI
Other	Z = -2.23, p = .027	n_A = 290, n_B = 290	App Collected More CI

In both tests, subjects using the application method collected more CII based on a 95 percent level of confidence. This indicates that the application is more likely to collect CII and the subject's familiarity with infrastructure deficiencies or their career field did not impact the results. However, it should be noted that the results (Z = -2.56, p < .027) of the grouping by "other" had a p-value that was close to the confidence coefficient (.05). This shows that there was significance at a 95 percent level of confidence. Whereas, the p-value (< .001) for the CE group was much lower. The later shows that there is significance at even a higher (99%) level of confidence. This indicates that CE subjects did report more CII and could be related to their assumed familiarity with reporting infrastructure issues.

Hypothesis Testing: Grouping by Subject's Familiarity With OPSEC

On the post-experiment questionnaire, subjects were asked to respond to the following question: "I understand the meaning of the term *Indicators of Critical Information* and how it relates to OPSEC". The subjects responded on a scale from 1 to 5, where 5 was strongly agree, and 1 was strongly disagree. This grouping method assumes that subjects who understood the term *OPSEC indicators* were more familiar with CII then subjects who were less familiar with the term. Therefore, the subjects were grouped together based their familiarity with OPSEC indicators. The subjects who answered with a 3 or greater were considered familiar and subjects with a response with less than 3 were considered less familiar with OPSEC and CII.

Another set of WTs was performed based on the grouping of familiarity with OPSEC. The results are presented in Table 14. Similar to the previous tests, the results show the application collecting significantly more CII that the traditional method for both groups. This indicates that the application collected more CII regardless of how familiar the subject was with OPSEC. It also indicates that users would require OPSEC training before using a mobile application to collect work order data. For the group that was not familiar with OPSEC, 10 participants used the application and 14 used the call-in method. For the group that was considered familiar with OPSEC, 10 participants used the application and 6 used the call-in method.

Table 14. Results of WT for Grouping by Familiarity With OPSEC Indicators

Familiar With OPSEC Indicators	**H_O: M_A-M_B = 0** **H_A: M_A > MB**	**Sample Size**	**Result**
No (<3)	$Z = -3.83$, $p < .001$	$n_A = 290$, $n_B = 406$	App Collected More CI
Yes (=>3)	$Z = -3.76$, $p < .001$	$n_A = 290$, $n_B = 174$	App Collected More CI

Confirming Results

In order to confirm the results, the analysis was re-accomplished using the Student's t-test rather than the WT. Even though the required assumption of normality was not satisfied, the Student's t-test is somewhat resilient to failure of that assumption (McClave, Benson, & Sincich, 2014). Using the same confidence coefficient (.05), the

Student's t-test produced identical end-results. The test statistics changed but the outcome or end result of the test was still the same. Fore example, Table 15 shows the results of the Student's t-test based on the grouping of familiarity with OPSEC. Comparing Table 15 to Table 14 shows the same outcome—subjects using the mobile application method collected significantly more CII than those using the traditional method. Every test that was previously conducted was re-accomplished using the Student's t-test and all the end-results matched the results of the WT.

Table 15. Results of Student's t-test for Grouping by Familiarity With OPSEC

Familiar With OPSEC Indicators	**H_O: M_A-M_B = 0** **H_A: M_A > M_B**	**Test Statistic**	**Degree of Freedom**	**Result**
No (<3)	$p < .001$	t = 4.40	df =491	App Collected More CI
Yes (=>3)	$p < .001$	t = 4.33	df =446	App Collected More CI

Finally, in the beginning of this chapter it was shown (Table 9) that 6 subjects with prior knowledge of the purpose of the experiment (collecting CII) collected, on average, less CII than subjects with no prior knowledge. Therefore, the initial "overall" WT was re-accomplished after removing the 6 subjects from the data. The result ($Z = -4.70$, $p < .001$) confirms that the application still collected more CII when the 6 subjects were removed. Therefore, the subjects with prior knowledge about the purpose of the experiment did not impact the overall results.

Conclusion

The Wilcoxon Ranked-Sum test was performed to compare the median of each group using an "overall" test and four different grouping methods. The overall test compared the response of the application to the response of the traditional method and showed that the application collected significantly more CII with a 95 percent level of confidence. The first grouping method was by location (Table 11), the second by potential CII (Table 12), the third by AFSC (Table 13), and the fourth by familiarity with OPSEC (Table 14). The results of all four of grouping methods showed that the application collected more CII than the traditional method.

The results were confirmed by re-accomplishing the statistical analysis for every WT performed using the Student's t-test. The p-values for the t-test change compared to the WT but the end results all stayed the same. Furthermore, the data was removed for the 6 subjects with prior-knowledge about the purpose of this research and the overall results did not change. Finally, the results of the statistical analysis confirm the research hypothesis—the application method captured more CII than the traditional method.

V. Discussion and Conclusion

Key Findings

The purpose of this research was to answer the question: *Does using a mobile application to collect work requests increase the risk of capturing critical information*? Based on the experimental results and the statistical analysis of those results. There is clear evidence suggesting that the use of a mobile application does increase the risk of collecting critical information. Therefore, if a mobile application is utilized to collect work requests, there should be risk mitigation process employed.

The first statistical test compared the results of the overall responses of the application versus the traditional method. The second test analyzed all 29 locations separately. At 9 of those locations the application collected more CII than the traditional method. For 1 of the 29 locations the phone collected more CII and the remaining 19 locations showed no significant difference between either method. A deeper look at each location shows the reasons why some locations did not show any difference between the two collection methods.

For the 9 locations that showed the application collecting more CII, the CII was in close proximity of the issue that was being reported. When the CII was close to the issue the application method had a greater chance of collecting CII when the subject submitted the required photo. Especially when participants took wide-angled photos to identify the problem or location. For example, at location 17 there was a building schematic (considered CII) on the wall next to a malfunctioning emergency HVAC shutdown switch. The map was only mentioned once in a phone conversation. However, eight participants captured the map in a wide-angled photo.

There was one location in which the call-in method collected significantly more CII than the application. The issue being reported was exposed electrical wiring connected to a 120-volt wall outlet that was located in a communications closet. When a subject identified the location as a "communications closet" it was considered CII. In this case the phone collected more CII because it was easy for subjects to describe the location over the phone but identifying the location as a communications closet was not required to accurately describe the location. For example, using the application, subjects would report the building and room number by typing it into the application. Likewise, subjects using the call-in method would report the building and room number but were more likely to verbally mention that it was a communications closet.

There were 19 locations that showed no difference between the two collection methods. For these locations there were three reasons for the results. Either the CII was not needed to describe the issue or location, the CII was pertinent to describing the issue or location or the CII was not in close proximity to the issue being reported. For example, at location 7 the entry door to the auditorium did not close properly and the location of the auditorium was considered CII (mass gathering location). The location of the auditorium was very relevant to describing the location of the issue. Therefore, subjects using both methods frequently referred the auditorium when submitting the work request.

There were 3 additional tests performed after grouping the data by potential CII, AFSC, and familiarity with OPSEC. The results of these three tests were all consistent and indicated that the application collected more CII than the traditional method.

Therefore, the results were not influenced by the amount of potential CII at each location, the subjects career field, or the subject's familiarity with OPSEC. However, since the subject familiarity with OPSEC did not impact the results, specific OPSEC training would be required before allowing the application to be used to real-world work order data.

Limitations of Current Research

A number of factors limit this research. During the experiment both methods only allowed one-way communication to a simulated CE customer service. Realistically, both methods would allow feedback from customer service. A question from customer service might have prompted a "real world" customer to disclose additional CII. For example, if a customer service representative were to request additional justification or a more detailed description of the location or issue. Furthermore, the application used during the experiment only allowed one photo to be submitted. Whereas, a more suitable mobile application would allow multiple photos and potentially video footage.

The AFIT campus facilities were used to conduct the experiment and the majority of the subjects were master's degree students attending AFIT. Only using one geographical location to conduct the experiment limits the types and amount of CII available for collection. For instance, collecting work requests around a mission critical facility, such as an Air Operations Center, may increase the availability of CII. Additionally, the subjects consisted of mostly company grade officers perusing a master's degree at AFIT. Therefore, the subjects represent a subgroup of the entire Air Force population of potential customers.

One-way communication, only allowing one photo submission, the use of only one geographical location, and subject diversity were all limitations of this research. A study that collects real world data at multiple geographical locations through the actually deployment of a more capable mobile application could overcome these limitations. However, this experiment still addresses the research question and shows an increased risk of collecting critical information when using a mobile application to collect work order data.

Recommendations for Action

One of the motivations for this research was to provide leaders with an evaluation of the OPSEC risks associated with using a mobile application to collect infrastructure deficiencies. The assumed benefits are that a mobile application would increase the effectiveness and efficiency of the work request collection process. Furthermore, deploying a mobile application would identify more infrastructure issues than the current process and that would help CE forecast a more accurate projection of the sustainment budget. This is based on the assumption that anyone with a mobile device and access to base would be able to report an issue. However, with more information being collected comes the accompanied risk of gathering more critical information. Therefore, a risk mitigations strategy and training plan needs to be developed prior to a full deployment of a mobile application.

The information can be protected through standard network security practices. A couple of ways to protect the information would be end-to-end encryption of the data being communicated, mandatory access security, and user authentication. Furthermore, the data should not be continuously stored on the mobile device, but rather transferred through a secured connection with a protected server. This way even if an adversary were to compromise a device, the information would be secure.

The current process is not perfectly secure. For example, some customers will take picture of a work request and email them to customer service. It is difficult to measure the frequency or the method in which customers transfer this information, but it can be assumed that in some cases mobile devices and personal email are being used. With a mobile application, the photos would be permitted but also regulated. For instance, if there is a particular area on base where photos should definitely not be permitted (e.g. flight line), the application knows the device location and can therefore limit particular types of submission based on that location.

Using a mobile application does come with increased risk. However, the risks can be managed by conducting some additional research and developing a mitigation strategy and training plan prior to deployment. Leaders should not hesitate to use mobile applications to collected work requests. Rather, the risks should be identified and managed.

Suggested Future Research

Deploying a mobile application to collect real-world work requests would be a better way to collect data for future analysis. The data could be used to measure effectiveness and efficiency of the application and evaluated for real world security issues. Furthermore, a controlled partial deployment of an application could measure an increase or decrease in work order submission as well as potential costs and savings.

The in-house development of a mobile application or the acquisition of a commercial-off-the-shelf product would be the first logical step. Then, the application could be provided to randomly selected facility managers or members of the Air Force community. It would still be vital to capture data related to the current process. Therefore, a well thought out methodology would be required. Approval to deploy such an application would likely be time consuming. Therefore future research would need to be broken into separate phases and leadership support would be essential.

Summary

This research was the first of its kind and used OPSEC principles to evaluate security concerns associated with using a mobile application to collect work order data. An experiment was used to compare a mobile application to the traditional collection process. The results of that experiment provide significant evidence that the use of a mobile application increases the risk of capturing critical information and indicators of critical information. Therefore, in order to deploy such an application there needs to be a risk mitigations strategy and methods in place to protect the information that would be collected.

Leadership support is needed to continue researching the risks and benefits of using a mobile application to submit work requests. The development or acquisition of a capable mobile application is needed for future research and the approval to conduct a limited and controlled real-world experiment is required. Potential benefits of continued research could be the eventual realization of increased effectiveness of the work order collection process, more reliable infrastructures, cost savings, protection of critical information, and a better projection of future sustainment budget requirements.

Appendix 1. Informed Consent Form

Consent to Participate in Research For Effects of Mobile Applications on the Traditional Work Order Submission Process

Principal Investigator: **Dr. Brent T. Langhals, DSN 785-3636, ext. 7402, AFIT/ENV**
brent.langhals@afit.edu

Associate Investigators: **Capt Victor Guinn, DSN 785-3636, ext. 7402, AFIT/ENV**
victor.guinn@afit.edu

Capt Michael Peterson, DSN 785-3636, ext. 7402, AFIT/ENV
michael.peterson@afit.edu

1. INTRODUCTION

You are being invited to take part in a research study. The information in this form is provided to help you decide whether or not to take part. Study personnel will be available to answer your questions and provide additional information. If you decide to take part in the study, you will be asked to sign this consent form. A copy of this form will be given to you. Your participation will occur at Wright Patterson AFB, OH.

2. PURPOSE

The purpose of this study is to determine if using a mobile application to collect civil engineering work requests is more or less efficient, effective, and secure then the current collection process. The intent of the study is to look at the pros and cons of incorporating a mobile application into the current work order submission process. The time requirement for each volunteer subject is anticipated to be a total of 30 consecutive minutes. It is expected that approximately 60 subjects will be enrolled in this study. Subjects must be able to speak, read, write, and understand English, talk on a telephone, operate an Android or IOS device, and see differences in colors.

3. PROCEDURES

If you decide to participate, you will be asked to complete a short post experiment questionnaire that will capture some demographic information and ask questions that cannot be revealed until after you participate in the experiment. Completing the questionnaire is completely voluntary. The demographic questions include the following:

1. How old are you?
2. What is your AFSC/Job Title?
3. What is your skill level?

4. What is your pay grade?

As part of the study, you will be asked to find and submit work order data that is located throughout the Air Force Institute of Technology Campus. There will be two types of submission methods: (1) Using a mobile application, (2) Using a telephone to call in work orders. If you choice to participate, you may be assigned both methods. You will be given a map and instructions that will show you where and how to identify and submit work requests.

Your participation in this study is voluntary. You will not lose any benefit that would normally be entitled if you do not participate or withdraw from the research. You may decide to not begin or to stop the study at any time. If you are a student, your refusing to participate will have no effect on your student status. Also, any new information discovered about the research will be provided to you. This information could affect your willingness to continue your participation and will therefore be furnished to you.

4. POTENTIAL RISKS and/or DISCOMFORTS

The tasks that you will be doing have no known safety or psychological risks. Although we have tried to avoid risks, if any discomfort occurs you can stop participating immediately.

5. PREGNANCY RISKS

There are no precautions for female subjects or subjects who are or may become pregnant during the course of this study.

6. BENEFITS

If you agree to take part in this research study there may be no direct benefit to you. However, the information learned from this study may someday help us improve the work order submission process.

7. COSTS

There will be no cost to you for the research study.

8. ALTERNATIVES TO PARTICIPATION

Your alternative is to choose not to participate in this research study. Refusal to participate will involve no penalty or loss of benefits to which you are otherwise entitled. You may discontinue participation at any time without penalty or loss of benefits to which you are otherwise entitled. You must notify one of the investigators of this study to discontinue.

9. YOUR PARTICIPATION IS VOLUNTARY

The decision to participate in this research is voluntary on your part. No one may coerce or intimidate you into participating in this program. Participate only if you want to. Dr Brent T Langhals, or an associate, should adequately answer all questions you have about this study, your participation and the procedures involved. If you have any further questions, Dr Langhals can be reached at (937) 255-3636 x7402. Dr. Langhals, or an associate will be available to answer any questions concerning procedures throughout this study. You may withdraw from this research study at any time without penalty.

If significant new findings develop during the course of this research, which may relate to your decision to continue participate or may affect the risk involved, you will be informed. Additionally, the investigator or Research Monitor of this study may terminate your participation in this study if she or he feels this to be in your best interest. If you have any questions or concerns about your participation in this study or your rights as a research subject, please contact the AFRL IRB at (937) 904-8100 or AFRL.IR.ProtocolManagement@us.af.mil.

If you are removed from the study, the study investigator will contact you to answer any questions you may have.

10. COMPENSATION

If you are active duty military you will receive your normal active duty pay. Additionally, as a courtesy you will be offered food and beverage after to you participate in this study.

11. RESEARCH-RELATED INJURY

Your entitlements to medical and dental care and/or compensation in the event of injury are governed by federal laws and regulations. If you desire further information you may contact the legal office (711 HPW/JA, 986--5666 at Wright-Patterson AFB). In the event of a research related injury, you may contact the Principal Investigator, Dr Brent T. Langhals, of this research study at (937) 255-3636).

12. SIGNIFICANT NEW FINDINGS

You will be told by the study investigator or study staff if new information becomes available that might affect your choice to stay in the study.

13. CONFIDENTIALITY

Records of your participation in this study may only be disclosed according to federal law, including the Federal Privacy Act, 5 U.S.C. 552a, and its implementing regulations and the Health Insurance Portability and Accountability Act (HIPAA), and its

implementing regulations, when applicable, and the Freedom of Information Act, 5 U.S.C. Sec 552, and its implementing regulations when applicable.
Your personal information will be stored in a locked cabinet in an office that is locked when not occupied. Electronic files containing your personal information will be password protected and stored only on a secure server. Organizations that may look at and/or copy your medical and/or records for research oversight, quality assurance and data analysis include:

1. the researchers named above,
2. the study's Research Monitor or Consultant,
3. the AFRL Wright Site IRB,
4. the Air Force Surgeon General's Research Compliance office,
5. the Director of Defense Research and Engineering office or
6. other IRB(s) involved in the review and approval of this protocol.

You will be identified by a code, and personal information from your records will not be released without your written permission unless required for military personnel. Information related to health and fitness for duty may be required to be reported to appropriate medical or command authorities. Complete confidentiality for military members cannot be promised. You will not be identified in any publication or in the sharing of your data about this study.

Your participation in this study may be audio recorded. The purpose of these recordings is capture a typical work order submission via telephone to then compare with work orders submitted via a mobile app.

Your personal information will be stored in a locked cabinet in an office that is locked when not occupied. Electronic files containing your personal information will be password protected and stored only on a secure server. It is intended that the only people having access to your information will be the researchers named above, the AFIT IRB or any other IRB involved in the review and approval of this protocol. When no longer needed for research purposes your information will be destroyed in a secure manner (shredding).

Complete confidentiality cannot be promised, in particular for military personnel, whose health or fitness for duty information may be required to be reported to appropriate medical or command authorities. If such information is to be reported, you will be informed of what is being reported and the reason for the report.

14. PRIVACY ACT

Personal Identifiable Information to be obtained for this study includes gender, job title, AFSC, skill level, age, and experience. Signing this document in no way alters your ability to obtain medical treatment that is not part of this study. If your data is disclosed by the investigator to one of the parties listed above, those parties may pass on your data without further notification to you. Data collected in the course of this study may be withheld from you by the investigator for the duration of the study. If withheld, your data will be released at the conclusion of the study.

15. STUDY PARTICIPATION AGREEMENT/CONSENT

Taking part in this research study is completely voluntary. Your signature below shows that:

1. You agree to be in this study
2. The researcher has explained the study to you and you have read and understand the information you have been given
3. You were given the opportunity to ask questions about the study and all of your questions
4. have been answered to your satisfaction
5. You understand that signing this consent does not take away any of your legal rights

You will be given a copy of this signed consent form for your records

Volunteer Signature _________________________________ Date _________

Volunteer Name (printed) ____________________________

Advising Investigator Signature _____________________________ Date __________

Investigator Name (printed) ___________________________

Witness Signature _________________________________ Date __________

Witness Name (printed) ______________________________

Privacy Act Statement

Authority: We are requesting disclosure of personal information. Researchers are authorized to collect personal information on research subjects under The Privacy Act-5 USC 552a, 10 USC 55, 10 USC 8013, 32 CFR 219, 45 CFR Part 46, and EO 9397, November 1943.

Purpose: It is possible that latent risks or injuries inherent in this experiment will not be discovered until some time in the future. The purpose of collecting this information is to aid researchers in locating you at a future date if further disclosures are appropriate.

Routine Uses: Information may be furnished to Federal, State and local agencies for any uses published by the Air Force in the Federal Register, 52 FR 16431, to include, furtherance of the research involved with this study and to provide medical care.

Disclosure: Disclosure of the requested information is voluntary. No adverse action whatsoever will be taken against you, and no privilege will be denied you based on the fact you do not disclose this information. However, your participation in this study may be impacted by a refusal to provide this information.

Appendix 2. Experiment Script

0:00 Participant arrives

"Welcome to testing of work order submission processes, today you will be testing smartphone or traditional work order submission. This test is voluntary and will last approximately 45-70 minutes. Upon completion refreshments will be offered. If you do not want to participate in this experiment then you may leave now or at any time during the experiment. If you wish to continue we will now be going over the informed consent form. Do you wish to continue?"

0:02 Have participant read and sign the Informed Consent Form

0:05 Experiment Description/Training

"This experiment simulates submitting a work order to a civil engineering squadron. The study consists of mostly an interior work order submission items, but will also consist of a temporary exterior portion that should only last 5-10 minutes. Throughout the AFIT complex we have identified a number of simulated and real world facility items that could be submitted to the facility manager or the civil engineering squadron to be replaced or repaired. We will identify these items by pointing to them. If you see a real world facility emergency that is not indicated by the researcher please notify the accompanying researcher. Under no circumstances are you to touch any facility infrastructure items during the experiment. If there are any questions during the course please ask the accompanying researcher. During the experiment if a real world emergency occurs please follow standard procedure regarding the particular emergency situation. If at any time you need to use the restroom please notify the accompanying researcher and utilize one of the restrooms along the route."

"Do you have any questions prior to training?"

0:07 Give training for smartphone and traditional

"All simulated work order submission items will be identified by the accompanying researcher. In some cases, the researcher will say a phrase about what the item is doing or not doing. During the experiment, you may ask the researcher if you are supposed to submit an item and point to it, they will respond with yes or point to the intended item. You may not ask what the item is or what is incorrect about it. For instance, we will show you a broken light, but not tell you what it is or how to describe it. All information that you submit must be from your own experience and interpretation from the phrase given by the researcher about the item. Are there any questions prior to instructions on the submission requirements?"

0:08 Traditional submission participants will be given this script portion

"You have been randomly selected to participate in traditional work order submission testing. You will follow the accompanying researcher through the work order submission course they will be present for questions relating to where you need to go and emergency procedure. To submit an item dial the following number 307-213-9677, the following message will play (*play message*). Please answer the questions after the tone. What is your subject number? What is your location? And what is the infrastructure problem that you are trying to submit? After the tone please answer the questions given by the message as if you were reporting an actual CE work order. Are there any questions? Are you ready to begin the course?"

(8:00) Smartphone submission participants will be given this script portion

"You have been randomly selected to participate in smartphone work order submission testing. You will follow the accompanying researcher through the work order submission course they will be present for questions relating to where you need to go and emergency procedure (*show individual how to use the application*). Open the application, select the submit icon (*open application, select submit*) fill in your subject number, fill in your location (*show individual how to do each step after saying it*). Select the camera and take a picture of the submission item (*show how to take a picture of the WO item*). If you feel like the picture doesn't describe the problem fully please add an additional description here; this is optional, all of the other fields are required (*show how to add additional description*). After filling out the form select the WO Submit button to submit the form. (*show how to submit the WO*). Please answer the questions on the smartphone as if you were reporting an actual CE work order. Are there any questions? Are you ready to begin the course?

10:00 Send participants through course with researcher

55:00 Ask participant to fill out post experiment questionnaire on computer

"Thank you for taking part in this test, would you please take a final post experiment questionnaire (*give individual the questionnaire on mobile computer*)."

70:00 After filling out the questionnaire

"Please do not talk to anyone about the experiment, until you are notified from the researcher that the results have been posted. If you have questions or concerns about the experiment you can address them now with the researcher, E-Mail, or call with the number provided (*give card with experiment contact information on it*)."

End: Offer participant courtesy food and beverage

Appendix 3. Post-Experiment Questionnaire

Responses to the following questions were collected using Google forms.

1. What is your subject number?
2. How old are you?
3. Are you color blind? (Yes/No)
4. What is your AFSC/Job Title?
5. What is your skill level?
6. What is your pay grade?
7. What is your gender? (Male/Female)
8. What is the highest degree or level of school you have completed or the highest degree you have received? (Less than a high school degree, High school degree or equivalent, Associate degree, Bachelor degree, Masters Degree, Doctorate degree)
9. Prior to participating in this study, I already knew that the study was investigating operational security (OPSEC)? (Yes/No)

Answer the following questions on a scale from 1 to 5. Where 1 is "Strongly Disagree" and 5 is "Strongly Agree".

10. Prior to participating in this study, I already knew that the study was investigating operational security (OPSEC) and because of that knowledge I tried to avoid collecting critical information.
11. I am familiar with the term Operational Security (OPSEC) and its meaning.
12. I have participated in Operational Security (OPSEC) training at least one time in my life.
13. I have participated in some type of Operational Security (OPSEC) training within the last 12 months.
14. I understand the meaning of the term "Critical Information" and how it relates to Operational Security (OPSEC).
15. I understand the meaning of the term "Indicators of Critical Information" and how it relates to Operational Security (OPSEC).

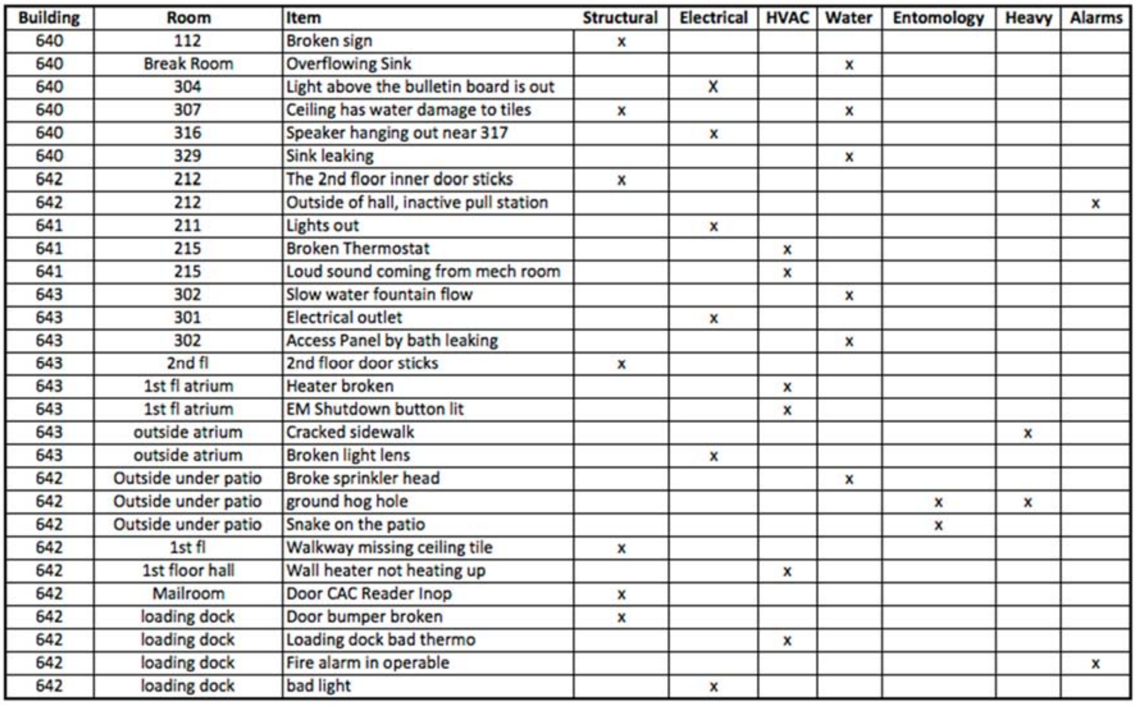
16. During the experiment, I was (at least once) concerned that I might be collecting Critical Information.

17. During the experiment, I was (at least once) concerned that I might be collecting Indicators of Critical Information.

18. During the experiment, I was (at least once) concerned about operational security.

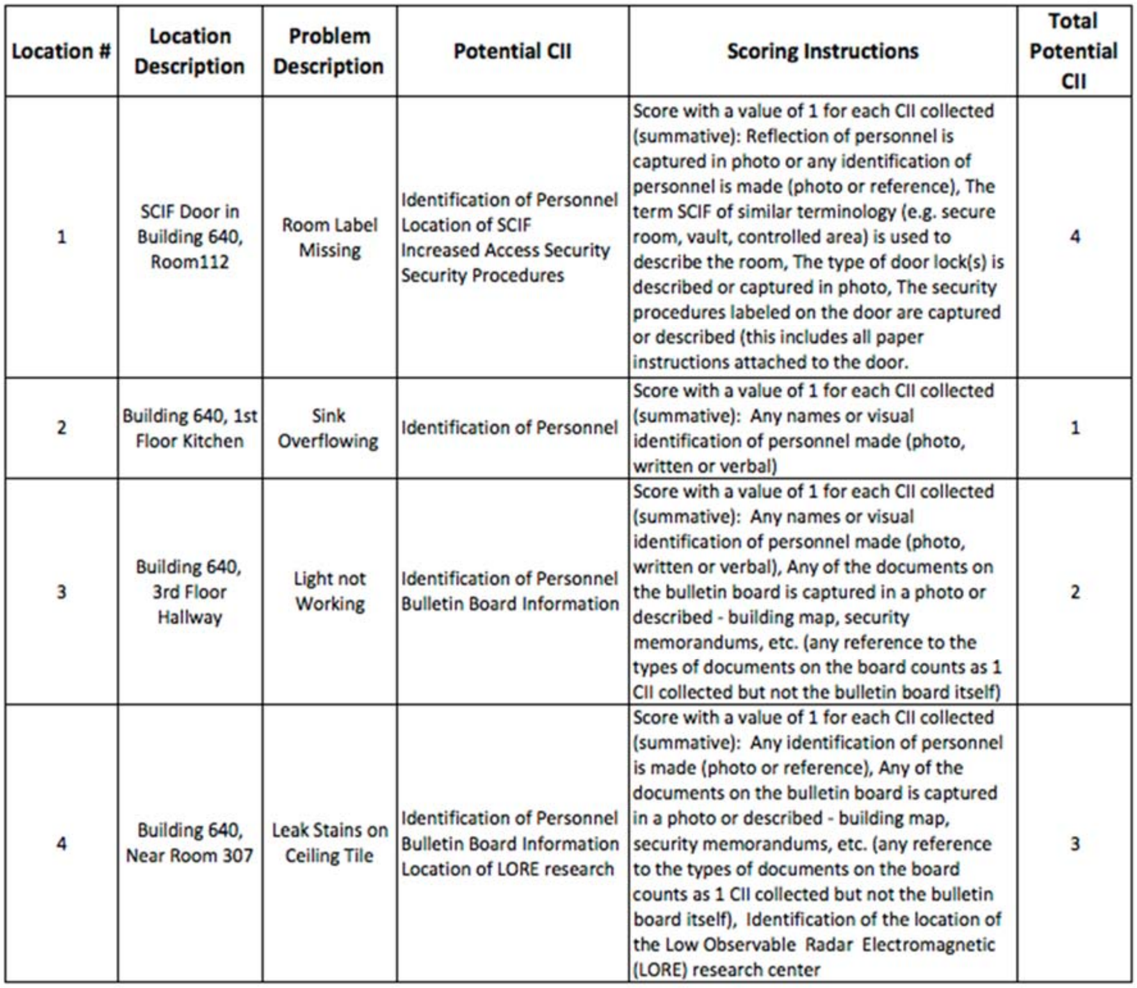
19. During the experiment, I collected and/or communicated Critical Information.

Appendix 4. Identified Work Requests

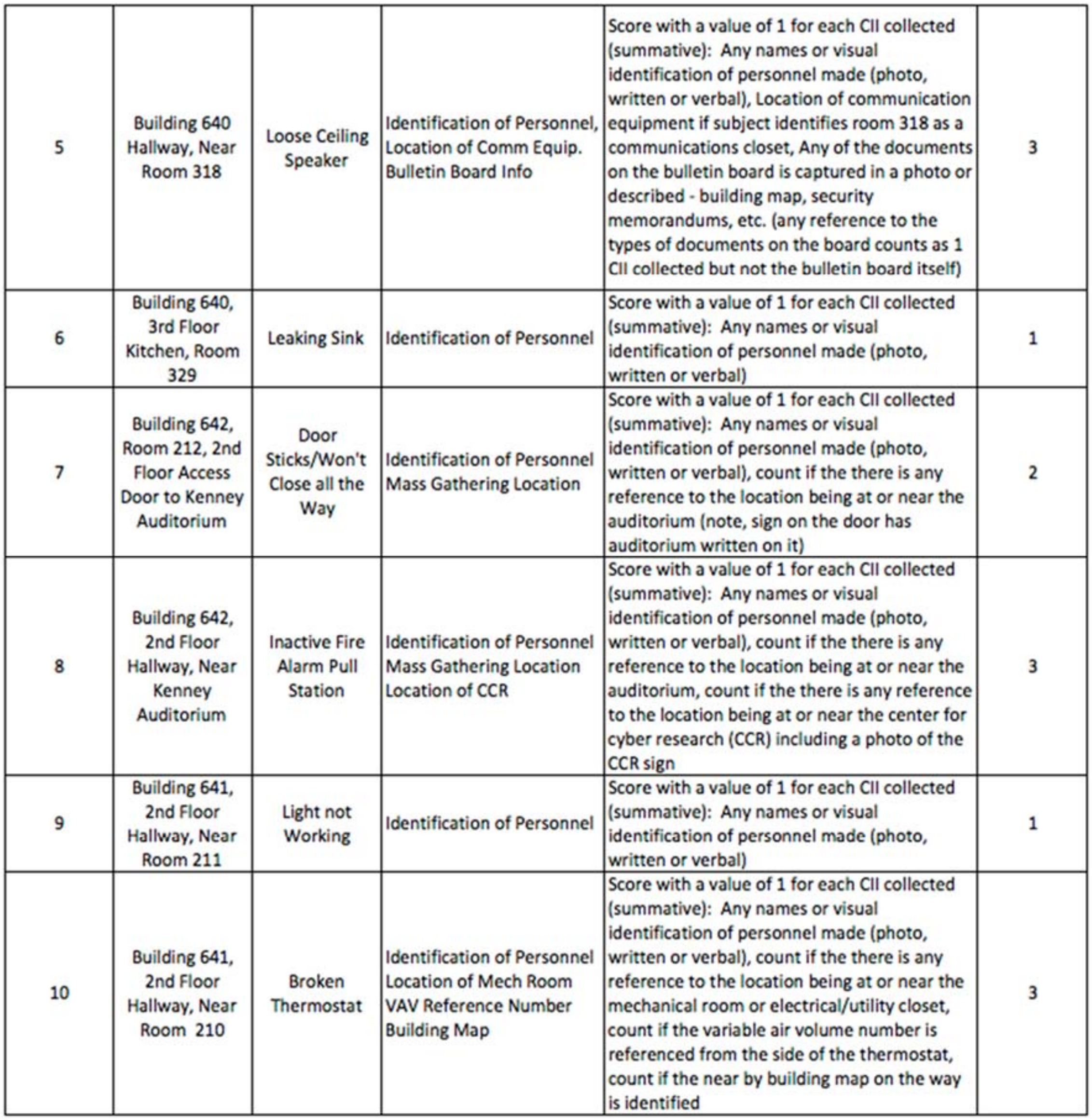


Building	Room	Item	Structural	Electrical	HVAC	Water	Entomology	Heavy	Alarms
640	112	Broken sign	x						
640	Break Room	Overflowing Sink				x			
640	304	Light above the bulletin board is out		X					
640	307	Ceiling has water damage to tiles	x			x			
640	316	Speaker hanging out near 317		x					
640	329	Sink leaking				x			
642	212	The 2nd floor inner door sticks	x						
642	212	Outside of hall, inactive pull station							x
641	211	Lights out		x					
641	215	Broken Thermostat			x				
641	215	Loud sound coming from mech room			x				
643	302	Slow water fountain flow				x			
643	301	Electrical outlet		x					
643	302	Access Panel by bath leaking				x			
643	2nd fl	2nd floor door sticks	x						
643	1st fl atrium	Heater broken			x				
643	1st fl atrium	EM Shutdown button lit			x				
643	outside atrium	Cracked sidewalk						x	
643	outside atrium	Broken light lens		x					
642	Outside under patio	Broke sprinkler head				x			
642	Outside under patio	ground hog hole					x	x	
642	Outside under patio	Snake on the patio					x		
642	1st fl	Walkway missing ceiling tile	x						
642	1st floor hall	Wall heater not heating up			x				
642	Mailroom	Door CAC Reader Inop	x						
642	loading dock	Door bumper broken	x						
642	loading dock	Loading dock bad thermo			x				
642	loading dock	Fire alarm in operable							x
642	loading dock	bad light		x					

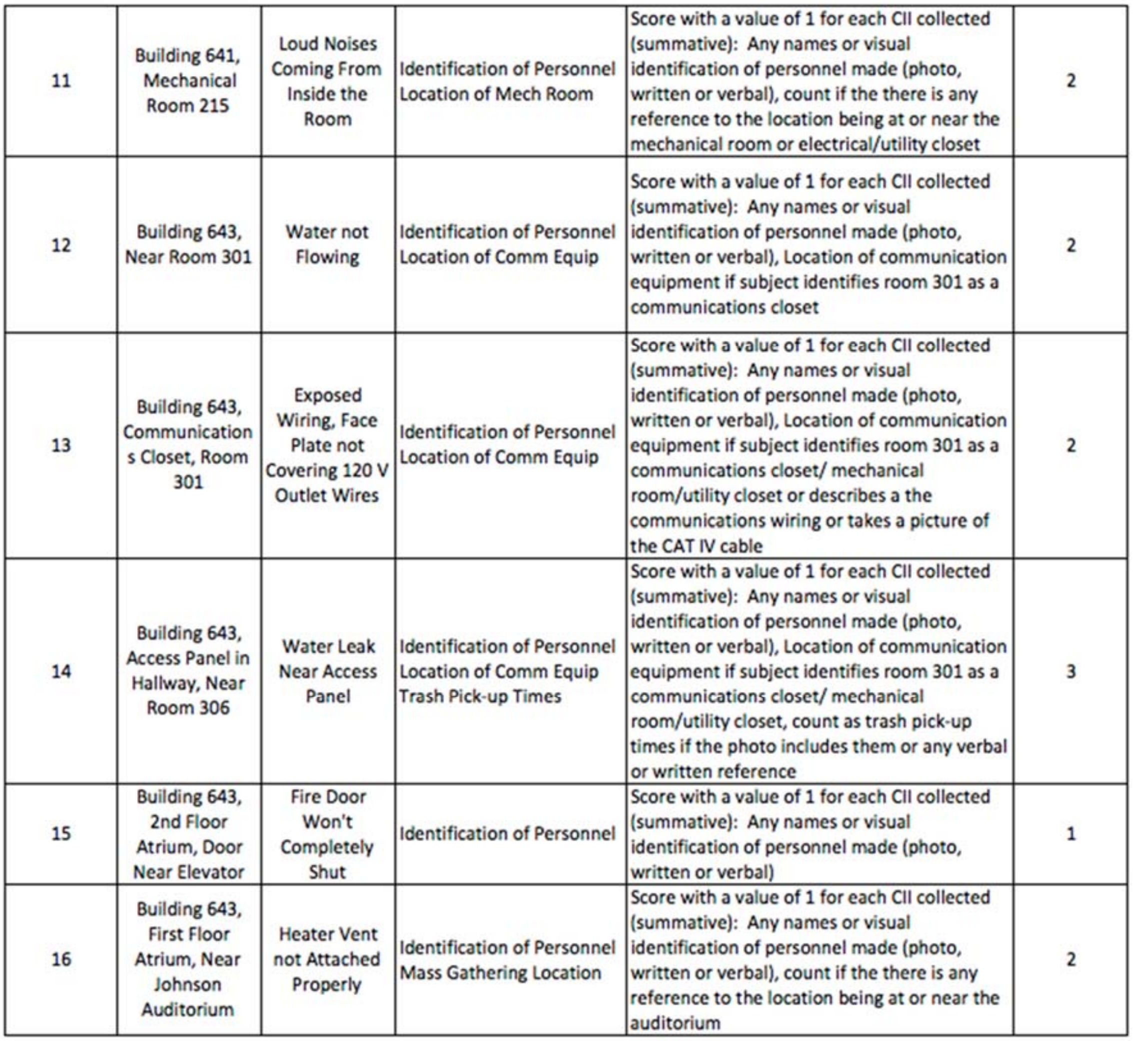
Appendix 5. Researcher's Grading Rubric



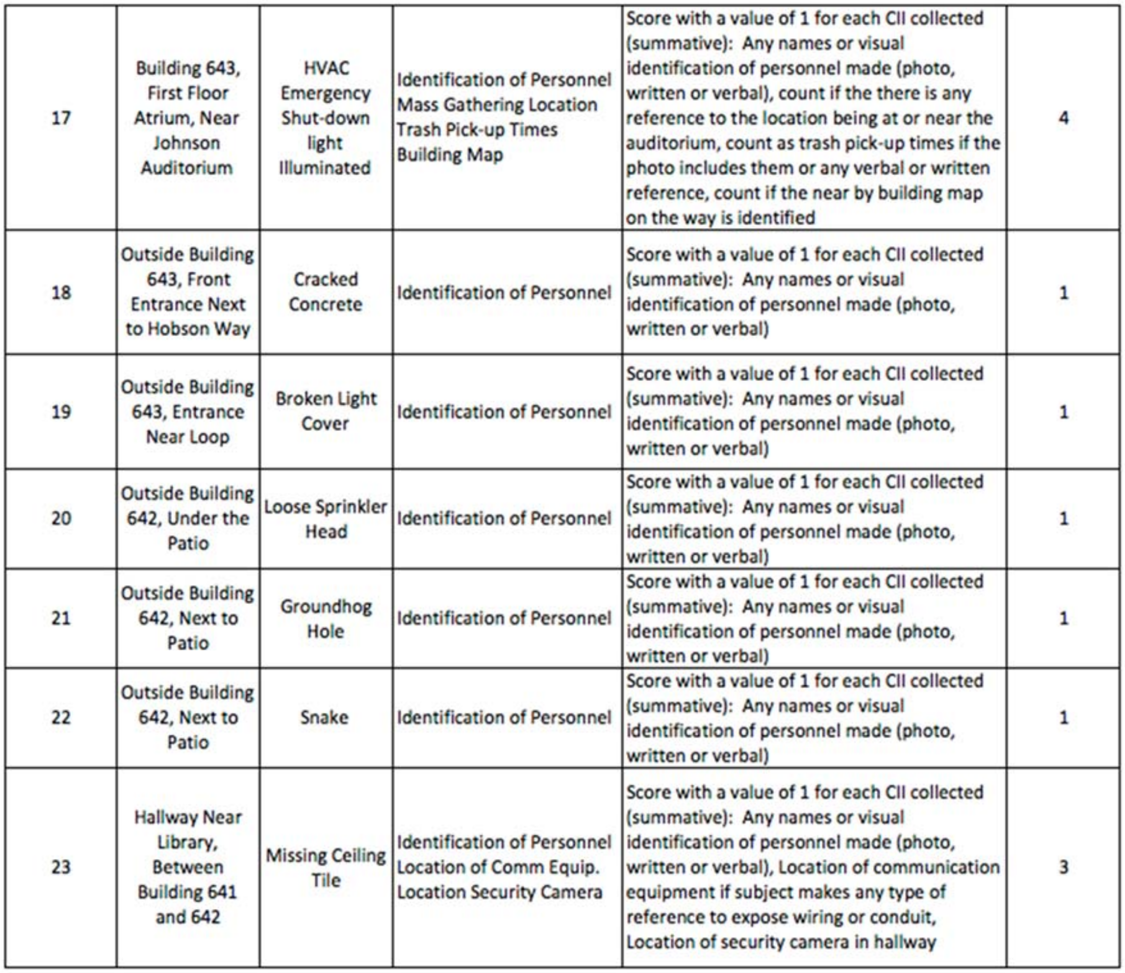
Location #	Location Description	Problem Description	Potential CII	Scoring Instructions	Total Potential CII
1	SCIF Door in Building 640, Room112	Room Label Missing	Identification of Personnel Location of SCIF Increased Access Security Security Procedures	Score with a value of 1 for each CII collected (summative): Reflection of personnel is captured in photo or any identification of personnel is made (photo or reference), The term SCIF of similar terminology (e.g. secure room, vault, controlled area) is used to describe the room, The type of door lock(s) is described or captured in photo, The security procedures labeled on the door are captured or described (this includes all paper instructions attached to the door.	4
2	Building 640, 1st Floor Kitchen	Sink Overflowing	Identification of Personnel	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal)	1
3	Building 640, 3rd Floor Hallway	Light not Working	Identification of Personnel Bulletin Board Information	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), Any of the documents on the bulletin board is captured in a photo or described - building map, security memorandums, etc. (any reference to the types of documents on the board counts as 1 CII collected but not the bulletin board itself)	2
4	Building 640, Near Room 307	Leak Stains on Ceiling Tile	Identification of Personnel Bulletin Board Information Location of LORE research	Score with a value of 1 for each CII collected (summative): Any identification of personnel is made (photo or reference), Any of the documents on the bulletin board is captured in a photo or described - building map, security memorandums, etc. (any reference to the types of documents on the board counts as 1 CII collected but not the bulletin board itself), Identification of the location of the Low Observable Radar Electromagnetic (LORE) research center	3



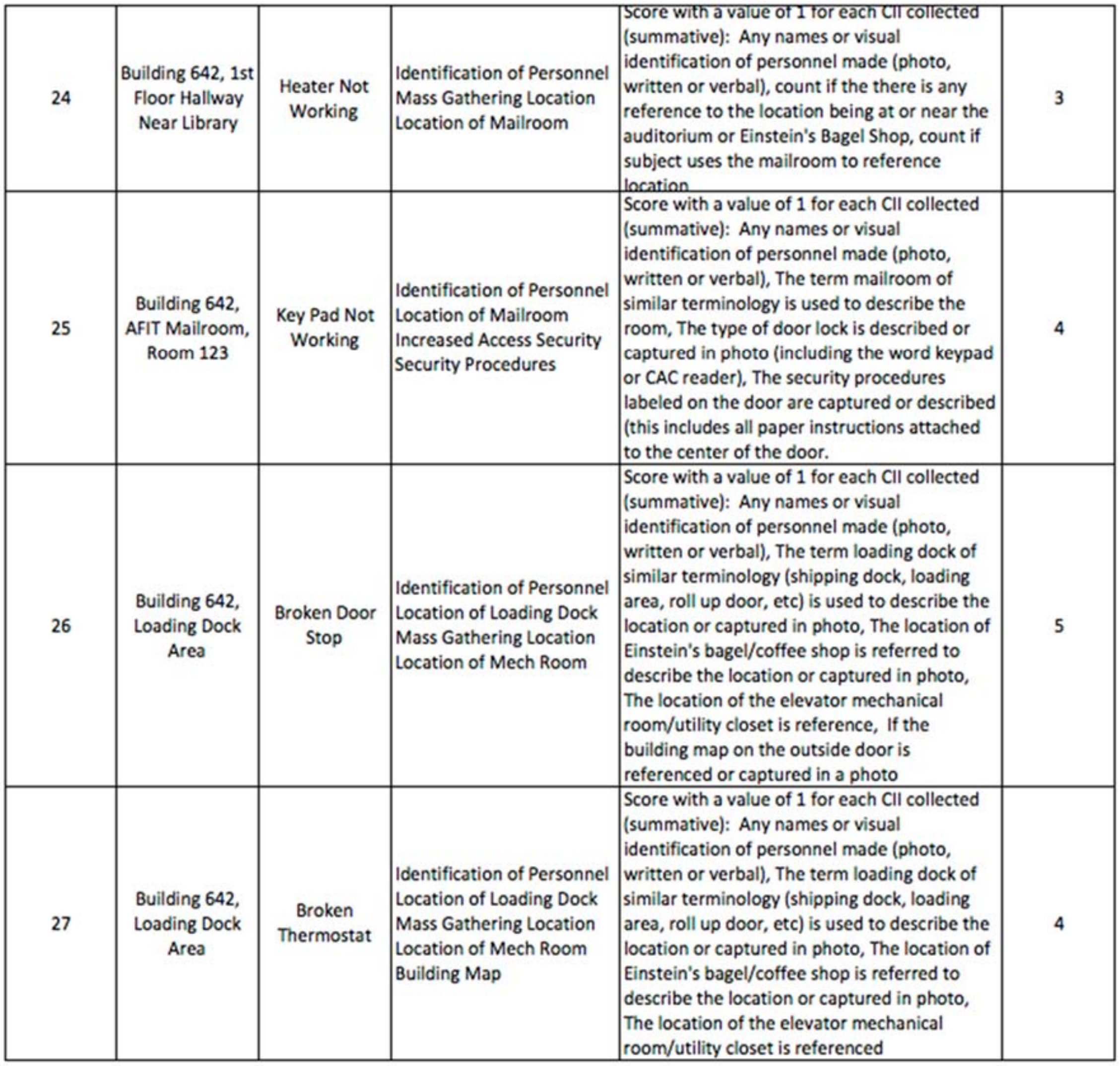
5	Building 640 Hallway, Near Room 318	Loose Ceiling Speaker	Identification of Personnel, Location of Comm Equip. Bulletin Board Info	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), Location of communication equipment if subject identifies room 318 as a communications closet, Any of the documents on the bulletin board is captured in a photo or described - building map, security memorandums, etc. (any reference to the types of documents on the board counts as 1 CII collected but not the bulletin board itself)	3
6	Building 640, 3rd Floor Kitchen, Room 329	Leaking Sink	Identification of Personnel	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal)	1
7	Building 642, Room 212, 2nd Floor Access Door to Kenney Auditorium	Door Sticks/Won't Close all the Way	Identification of Personnel Mass Gathering Location	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), count if the there is any reference to the location being at or near the auditorium (note, sign on the door has auditorium written on it)	2
8	Building 642, 2nd Floor Hallway, Near Kenney Auditorium	Inactive Fire Alarm Pull Station	Identification of Personnel Mass Gathering Location Location of CCR	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), count if the there is any reference to the location being at or near the auditorium, count if the there is any reference to the location being at or near the center for cyber research (CCR) including a photo of the CCR sign	3
9	Building 641, 2nd Floor Hallway, Near Room 211	Light not Working	Identification of Personnel	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal)	1
10	Building 641, 2nd Floor Hallway, Near Room 210	Broken Thermostat	Identification of Personnel Location of Mech Room VAV Reference Number Building Map	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), count if the there is any reference to the location being at or near the mechanical room or electrical/utility closet, count if the variable air volume number is referenced from the side of the thermostat, count if the near by building map on the way is identified	3



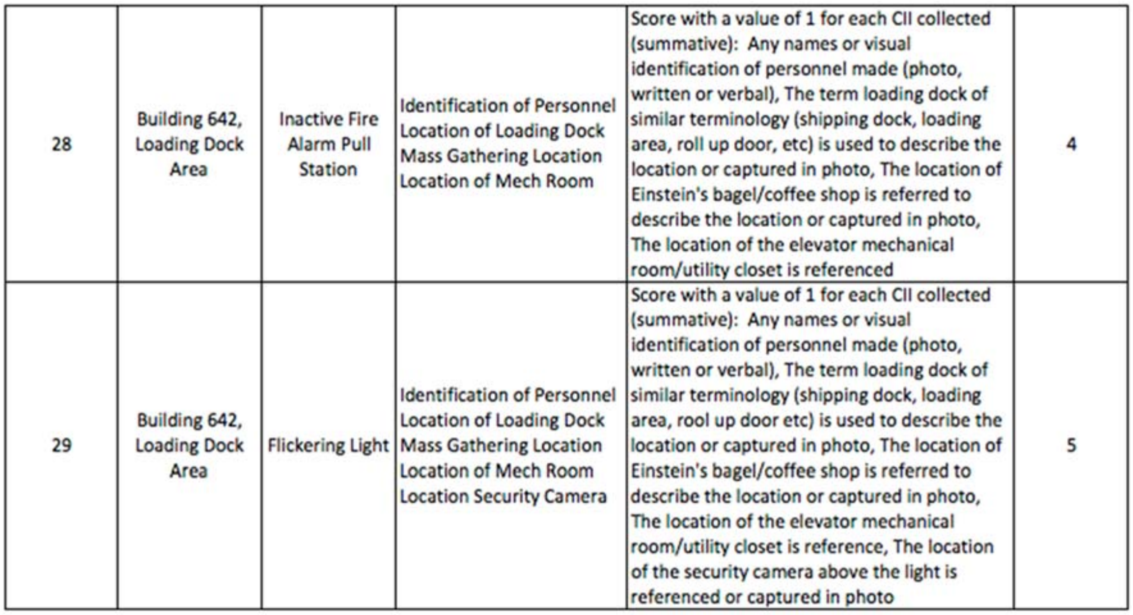
11	Building 641, Mechanical Room 215	Loud Noises Coming From Inside the Room	Identification of Personnel Location of Mech Room	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), count if the there is any reference to the location being at or near the mechanical room or electrical/utility closet	2
12	Building 643, Near Room 301	Water not Flowing	Identification of Personnel Location of Comm Equip	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), Location of communication equipment if subject identifies room 301 as a communications closet	2
13	Building 643, Communications Closet, Room 301	Exposed Wiring, Face Plate not Covering 120 V Outlet Wires	Identification of Personnel Location of Comm Equip	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), Location of communication equipment if subject identifies room 301 as a communications closet/ mechanical room/utility closet or describes a the communications wiring or takes a picture of the CAT IV cable	2
14	Building 643, Access Panel in Hallway, Near Room 306	Water Leak Near Access Panel	Identification of Personnel Location of Comm Equip Trash Pick-up Times	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), Location of communication equipment if subject identifies room 301 as a communications closet/ mechanical room/utility closet, count as trash pick-up times if the photo includes them or any verbal or written reference	3
15	Building 643, 2nd Floor Atrium, Door Near Elevator	Fire Door Won't Completely Shut	Identification of Personnel	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal)	1
16	Building 643, First Floor Atrium, Near Johnson Auditorium	Heater Vent not Attached Properly	Identification of Personnel Mass Gathering Location	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), count if the there is any reference to the location being at or near the auditorium	2



17	Building 643, First Floor Atrium, Near Johnson Auditorium	HVAC Emergency Shut-down light Illuminated	Identification of Personnel Mass Gathering Location Trash Pick-up Times Building Map	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), count if the there is any reference to the location being at or near the auditorium, count as trash pick-up times if the photo includes them or any verbal or written reference, count if the near by building map on the way is identified	4
18	Outside Building 643, Front Entrance Next to Hobson Way	Cracked Concrete	Identification of Personnel	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal)	1
19	Outside Building 643, Entrance Near Loop	Broken Light Cover	Identification of Personnel	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal)	1
20	Outside Building 642, Under the Patio	Loose Sprinkler Head	Identification of Personnel	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal)	1
21	Outside Building 642, Next to Patio	Groundhog Hole	Identification of Personnel	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal)	1
22	Outside Building 642, Next to Patio	Snake	Identification of Personnel	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal)	1
23	Hallway Near Library, Between Building 641 and 642	Missing Ceiling Tile	Identification of Personnel Location of Comm Equip. Location Security Camera	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), Location of communication equipment if subject makes any type of reference to expose wiring or conduit, Location of security camera in hallway	3



24	Building 642, 1st Floor Hallway Near Library	Heater Not Working	Identification of Personnel Mass Gathering Location Location of Mailroom	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), count if the there is any reference to the location being at or near the auditorium or Einstein's Bagel Shop, count if subject uses the mailroom to reference location	3
25	Building 642, AFIT Mailroom, Room 123	Key Pad Not Working	Identification of Personnel Location of Mailroom Increased Access Security Security Procedures	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), The term mailroom of similar terminology is used to describe the room, The type of door lock is described or captured in photo (including the word keypad or CAC reader), The security procedures labeled on the door are captured or described (this includes all paper instructions attached to the center of the door.	4
26	Building 642, Loading Dock Area	Broken Door Stop	Identification of Personnel Location of Loading Dock Mass Gathering Location Location of Mech Room	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), The term loading dock of similar terminology (shipping dock, loading area, roll up door, etc) is used to describe the location or captured in photo, The location of Einstein's bagel/coffee shop is referred to describe the location or captured in photo, The location of the elevator mechanical room/utility closet is reference, If the building map on the outside door is referenced or captured in a photo	5
27	Building 642, Loading Dock Area	Broken Thermostat	Identification of Personnel Location of Loading Dock Mass Gathering Location Location of Mech Room Building Map	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), The term loading dock of similar terminology (shipping dock, loading area, roll up door, etc) is used to describe the location or captured in photo, The location of Einstein's bagel/coffee shop is referred to describe the location or captured in photo, The location of the elevator mechanical room/utility closet is referenced	4



28	Building 642, Loading Dock Area	Inactive Fire Alarm Pull Station	Identification of Personnel Location of Loading Dock Mass Gathering Location Location of Mech Room	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), The term loading dock of similar terminology (shipping dock, loading area, roll up door, etc) is used to describe the location or captured in photo, The location of Einstein's bagel/coffee shop is referred to describe the location or captured in photo, The location of the elevator mechanical room/utility closet is referenced	4
29	Building 642, Loading Dock Area	Flickering Light	Identification of Personnel Location of Loading Dock Mass Gathering Location Location of Mech Room Location Security Camera	Score with a value of 1 for each CII collected (summative): Any names or visual identification of personnel made (photo, written or verbal), The term loading dock of similar terminology (shipping dock, loading area, rool up door etc) is used to describe the location or captured in photo, The location of Einstein's bagel/coffee shop is referred to describe the location or captured in photo, The location of the elevator mechanical room/utility closet is reference, The location of the security camera above the light is referenced or captured in photo	5

References

Anderson, Mark J., & Kraber, Shari L. (2002). Keys to successful designed experiments. Retrieved May 25th, 2016 from http://www.isixsigma.com/tt/doe/.

Cohen, J. (1992). A power primer. *Psychological Bulletin*, 112(1), 155-159. doi:10.1037/0033-2909.112.1.155

Collins, H. (2011). Fixing by clicking. *Government Technology*, 24(11), 26–27.

Daft, R., & Lengel, R. (1986). Organizational information requirements, media richness and structural design. Management Science, 32(5), 554–571.http://doi.org/10.1287/mnsc.32.5.554.

Davis, J. E. (2013). 30TH Space Wing Instruction 32-1001. Vandenberg AFB. Retrieved from http://www.e-publishing.af.mil

Department of Defense (2006). *DoD Operations Security (OPSEC) Program*. Directive 5205.02. Washington, DC: Department of Defense.

Department of the Air Force (2011). *Operations Security (OPSEC).* Air Force Instruction 10-701. Washington, DC: HQ AF/A3Z-CI.

Eulberg, D. (2007). Transforming the way we work. *Air Force Civil Engineer*, 15(5), 2. Retrieved from http://www.afcec.af.mil/shared/media/document/AFD-120926 124.pdf.

Files, L. B. (2009). Treasury's role as the custodian of value for intellectual property and critical information: The impact of operational security on valuation. *Journal of Corporate Treasury Management*, 2(4), 298–311. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=44306835&lag=pt-br&site=ehost-live.

Giles, L. (1910). *Sun Tzu on the Art of War*. Allandale Online Publishing. Retrieved from https://www.ualberta.ca/~enoch/Readings/The_Art_Of_War.pdf.

Hasberry, V. L. (1991). Base Civil Engineer Work Request (32 No. 332). Arlington. Retrieved from http://www.e-publishing.af.mil

Hatch, D. (1993). Purple dragon: The origin and development of the United States OPSEC program. *Cryptologic Quarterly*, 2(6), 1–99. Retrieved from https://www.nsa.gov/public_info/_files/cryptologic_quarterly/purple_dragon.pdf.

Joyner, A. (2010). For making it easy to be a good citizen. *Inc.*, 32(10), 100.

Lengel, R. H., & Daft, R. L. (1988). The selection of communication media as an executive skill. *Academy Of Management Executive*, 2(3), 225–232. http://doi.org/10.5465/AME.1988.4277259.

Office of the National Counterintelligence Executive (2003). *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage–2002.* Washington, DC: NCIX.

McClave, J. T., Benson, P. G., & Sincich, T. (2014). *Statistics for business and economics* (12th ed.). Boston: Pearson.

Patten, M. L. (2009). *Understanding research methods: An overview of the essentials.* Glendale, CA: Pyrczak Pub.

Pattokos, A. (1999). The operations security connection. *Program Manager*, 28(1), 36-38. Retrieved from http://www.au.af.mil/au/awc/awcgate/dau/pattakjf.pdf.

Sørensen, C., Al-Taitoon, A., Kietzman, J., Pica, D., Wiredu, G. O., Elaluf-Calderwood, S., … Gibson, D. (2008). Exploring enterprise mobility: Lessons from the field. *Information Knowledge Systems Management*, 7, 243–271. Retrieved from http://eprints.lse.ac.uk/28387/.

Traynor, P., Amrutkar, C., Rao, V., Jaeger, T., McDaniel, P., & Porta, T. L. (2011). From mobile phones to responsible devices. *Security & Communication Networks*, 4(6), 719–726. http://doi.org/10.1002/sec.218.

U.S. Joint Chiefs of Staff (2006). *Operations Security*. Joint Publication 3-13.3. Washington, DC: U.S. Joint Chiefs of Staff

Vita

Captain Michael Peterson graduated from Hampton High School in Hampton, Tennessee. In November 2005 he enlisted in the Air Force and worked as a Material Management Journeyman until he was accepted into the Airmen education and commissioning (AECP) program in September 2009. As part of the commissioning program, he attended the University of Tennessee and graduated cum laude with a Bachelors of Science in Electrical Engineering. In August 2012 he completed basic officer training at Maxwell Air Force Base and commissioned as a Second Lieutenant in the United States Air Force.

His first officer duty station was to the 786th Civil Engineering Squadron, Ramstein Air Force Base, Germany where he was assigned the duties of Operations Engineering Deputy, Squadron Section Commander, and Chief of Portfolio Optimization. He was chosen to complete his Master of Science degree in Engineering Management at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio where he is expected to graduate in March 2017. Following his graduation, Captain Peterson will be assigned to the 45th Civil Engineer Squadron, Patrick Air Force Base, Florida.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)* 23-03-2017	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From – To)* Sept 2015 – March 2017

TITLE AND SUBTITLE The Security Risks Associated With Using a Mobile Application to Collect Work Order Data	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Peterson, Michael W., Captain, USAF	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/ENY) 2950 Hobson Way, Building 640 WPAFB OH 45433-8865	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT-ENV-MS-17-M-213
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Intentionally left blank	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRUBTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

The use of smart phone technology may be able to improve the Air Force's ability to sustain infrastructure, reduce costs and redundancy, and provide a more accurate sustainment budget forecast by using a mobile application to collect infrastructure deficiencies. However, before any such benefits can be realized, Air Force leaders need to know the security risks associated with the implementation of mobile technology. According to Daft and Lengel (1986), "information richness is defined as the ability of information to change understanding within a time interval" (p. 560). The "richer" the communication medium, the more effective it is at changing understanding. Based on media richness theory, a mobile application may be considered a "richer" form of communication. With additional richness and consequently more learning, are unintended operational security (OPSEC) cues transmitted via a mobile application as compared to traditional work order submission methods? This uses OPSEC principles to evaluate security concerns associated with using a mobile application to collect work order data. An experiment was conducted to compare a mobile application to the traditional collection process. The results of that experiment provide significant evidence that the use of a mobile application increases the risk of capturing critical information.

15. SUBJECT TERMS
Operational Security, Critical Information, Work Order, Mobile Applications, Technology

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Dr. Brent T. Langhals, AFIT/ENV
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	92	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 7402 brent.langhals@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18